

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

CPC PATENT TECHNOLOGIES PTY LTD.,
Patent Owner/Appellant

v.

Appeal Nos. 2024-1492¹
2024-1493

ASSA ABLOY AB, ASSA ABLOY INC.,
ASSA ABLOY RESIDENTIAL GROUP, INC.,
AUGUST HOME, INC., HID GLOBAL CORP.,
ASSA ABLOY GLOBAL SOLUTIONS, INC.,
Petitioners/Appellees

Proceeding Nos.: IPR2022-01093 and IPR2022-01094

NOTICE FORWARDING CERTIFIED LIST

A Notice of Appeal to the United States Court of Appeals for the Federal Circuit was timely filed February 15, 2024, in the United States Patent and Trademark Office in connection with the above identified *Inter Partes Review* proceedings. Pursuant to 35 U.S.C. § 143, a Certified List is this day being forwarded to the Federal Circuit.

Respectfully submitted,

Date: March 26, 2024

By: Macia L. Fletcher
Macia L. Fletcher
Paralegal
Mail Stop 8
P.O. Box 1450
Alexandria, Virginia 22313-1450
(571) 272-9035

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

¹ Appeal No. 2024-1492 (Lead) is consolidated with Appeal No. 2024-1493 (Member Case) pursuant to Court Order (Dkt. No. 13) and Note to File (Dkt. No. 14) dated March 6, 2024.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing NOTICE FORWARDING CERTIFIED LIST has been served, via electronic mail, on counsel for Appellant and Appellees this 26th day of March, 2024, as follows:

<u>PATENT OWNER:</u>	<u>PETITIONERS:</u>
Steven M. Coyle Nicholas Geiger Andrew C. Ryan Michael J. Rye CANTOR COLBURN LLP scoyle@cantorcolburn.com NGeiger@CantorColburn.com ryan@cantorcolburn.com mrye@cantorcolburn.com	Lionel M. Lavenue Jonathan J. Fagan Benjamin Aaron Saidman Kara Allyse Specht FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP lionel.lavenue@finnegan.com jonathan.fagan@finnegan.com benjamin.saidman@finnegan.com kara.specht@finnegan.com

By: Macia L. Fletcher

Macia L. Fletcher
Paralegal
Mail Stop 8
P.O. Box 1450
Alexandria, Virginia 22313-1450
(571) 272-9035

U.S. DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

March 26, 2024

(Date)

THIS IS TO CERTIFY that the attached document is a list of the papers that comprise the record before the Patent Trial and Appeal Board (PTAB) for the *Inter Partes Review* proceeding identified below.

**ASSA ABLOY AB, ASSA ABLOY INC.,
ASSA ABLOY RESIDENTIAL GROUP, INC., AUGUST HOME, INC.,
HID GLOBAL CORPORATION, and
ASSA ABLOY GLOBAL SOLUTIONS, INC.,
Petitioner,**

v.

**CPC PATENT TECHNOLOGIES PTY, LTD.,
Patent Owner.**

**Case: IPR2022-01093
Patent No. 8,620,039 B2
By authority of the**

**DIRECTOR OF THE UNITED STATES
PATENT AND TRADEMARK OFFICE**

Macia L. Fletcher

Certifying Officer



Prosecution History ~ IPR2022-01093

Date	Document
6/13/2022	Petition for Inter Partes Review
6/13/2022	Petitioners' Power of Attorney
6/13/2022	Petitioners' Ranking and Explanation for Two Petitions Challenging U.S. Patent No. 8,620,039
7/29/2022	Patent Owner's Power of Attorney
7/29/2022	Patent Owner's Mandatory Notices
8/4/2022	Notice of Filing Date Accorded to Petition and Time for Filing Patent Owner's Preliminary Response
10/26/2022	Patent Owner's Exhibit List
10/26/2022	Motion for Pro Hac Vice Admission - Geiger
10/26/2022	Motion for Pro Hac Vice Admission - Coyle
11/3/2022	Order - Pro Hac Vice Admission - Coyle and Geiger
11/4/2022	Joint Motion for Protective Order
11/4/2022	Patent Owner's Exhibit List
11/4/2022	Patent Owner's Preliminary Response
11/17/2022	Revised Joint Motion for Protective Order
12/21/2022	Petitioners' Updated Exhibit List
12/21/2022	Petitioners' Reply to Patent Owner's Preliminary Response
1/6/2023	Petitioners' Updated Mandatory Notices
1/11/2023	Patent Owner's Sur-Reply to Petitioners' Preliminary Response Reply
2/2/2023	Scheduling Order
2/2/2023	Decision - Institution of Inter Partes Review
4/5/2023	Joint Notice of Stipulation Regarding Modification of Due Dates 1, 2, and 3
4/17/2023	Notice of Deposition - Lipoff
5/11/2023	Patent Owner's Response
6/22/2023	Notice of Deposition - Russ, Ph.D.
7/28/2023	Petitioners' Updated Exhibit List
7/28/2023	Petitioners' Reply to Patent Owner's Response
8/21/2023	Second Notice of Deposition - Lipoff
9/8/2023	Patent Owner's Sur-Reply
9/8/2023	Amended Scheduling Order
9/14/2023	Petitioners' Request for Oral Argument
9/14/2023	Patent Owner's Request for Oral Argument
10/31/2023	Order - Requests for Oral Argument
11/6/2023	Petitioners' Updated Exhibit List
11/7/2023	Patent Owner's Updated Exhibit List
1/31/2024	Final Written Decision
2/1/2024	Oral Hearing Transcript

U.S. DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

March 26, 2024

(Date)

THIS IS TO CERTIFY that the attached document is a list of the papers that comprise the record before the Patent Trial and Appeal Board (PTAB) for the *Inter Partes Review* proceeding identified below.

**ASSA ABLOY AB, ASSA ABLOY INC.,
ASSA ABLOY RESIDENTIAL GROUP, INC., AUGUST HOME, INC.,
HID GLOBAL CORPORATION, and
ASSA ABLOY GLOBAL SOLUTIONS, INC.,
Petitioner,**

v.

**CPC PATENT TECHNOLOGIES PTY, LTD.,
Patent Owner.**

**Case: IPR2022-01094
Patent No. 8,620,039 B2
By authority of the**

**DIRECTOR OF THE UNITED STATES
PATENT AND TRADEMARK OFFICE**

Macia L. Fletcher

Certifying Officer



Prosecution History ~ IPR2022-01094

Date	Document
6/13/2022	Petition for Inter Partes Review
6/13/2022	Petitioners' Power of Attorney
6/13/2022	Petitioners' Ranking and Explanation for Two Petitions Challenging U.S. Patent No. 8,620,039
7/29/2022	Patent Owner's Power of Attorney
7/29/2022	Patent Owner's Mandatory Notices
8/4/2022	Notice of Filing Date Accorded to Petition and Time for Filing Patent Owner's Preliminary Response
10/26/2022	Patent Owner's Exhibit List
10/26/2022	Motion for Pro Hac Vice Admission - Geiger
10/26/2022	Motion for Pro Hac Vice Admission - Coyle
11/3/2022	Order - Pro Hac Vice Admission - Coyle and Geiger
11/4/2022	Joint Motion for Protective Order
11/4/2022	Patent Owner's Exhibit List
11/4/2022	Patent Owner's Preliminary Response
11/17/2022	Revised Joint Motion for Protective Order
12/21/2022	Petitioners' Updated Exhibit List
12/21/2022	Petitioners' Reply to Patent Owner's Preliminary Response
1/6/2023	Petitioners' Updated Mandatory Notices
1/11/2023	Patent Owner's Sur-Reply to Petitioners' Preliminary Response Reply
2/2/2023	Scheduling Order
2/2/2023	Decision - Institution of Inter Partes Review
4/5/2023	Joint Notice of Stipulation Regarding Modification of Due Dates 1, 2 and 3
4/17/2023	Notice of Deposition - Lipoff
5/11/2023	Patent Owner's Response
6/22/2023	Notice of Deposition - Russ, Ph.D.
7/28/2023	Petitioners' Updated Exhibit List
7/28/2023	Petitioners' Reply to Patent Owner's Response
8/21/2023	Second Notice of Deposition - Lipoff
9/8/2023	Patent Owner's Sur-Reply
9/8/2023	Amended Scheduling Order
9/14/2023	Petitioners' Request for Oral Argument
9/14/2023	Patent Owner's Request for Oral Argument
10/31/2023	Order - Requests for Oral Argument
11/6/2023	Petitioners' Updated Exhibit List
11/7/2023	Patent Owner's Updated Exhibit List
1/31/2024	Final Written Decision
2/1/2024	Oral Hearing Transcript

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASSA ABLOY AB, ASSA ABLOY INC.,
ASSA ABLOY RESIDENTIAL GROUP, INC., AUGUST HOME, INC.,
HID GLOBAL CORPORATION, and
ASSA ABLOY GLOBAL SOLUTIONS, INC.,
Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY, LTD,
Patent Owner.

IPR2022-01093
Patent No. 8,620,039 B2

Before SCOTT A. DANIELS, AMBER L. HAGY and
FREDERICK C. LANEY, *Administrative Patent Judges*.

DANIELS, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

IPR2022-01093
Patent 8,620,039 B2

I. INTRODUCTION

ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global Corporation, and ASSA ABLOY Global Solutions, Inc., (“ASSA” or “Petitioner”) filed a Petition requesting *inter partes* review (“IPR”) of claims 1, 2, 13, 14, 19, and 20 of U.S. Patent No. 8,620,039 B2 (Ex. 1001, “the ’039 patent”). Paper 2 (“Pet”). CPC Patent Technologies PTY, Ltd, (“CPC” or “Patent Owner”) filed a Preliminary Response to the Petition. Paper 12 (“Prelim. Resp.”). With our email authorization, Petitioner filed a Reply to Patent Owner’s Preliminary Response. Paper 16 (“Prelim. Reply”). Also with our authorization, Patent Owner filed a Sur-Reply to Petitioner’s Reply. Paper 19 (“Prelim. Sur-Reply”).

Following our Institution Decision (Paper 20, “Inst. Dec.”), in which we determined that Petitioner was *not* time-barred from filing its Petition, Patent Owner filed a Response. Paper 24 (“PO Resp.”). *See* Inst. Dec. 9–34. Petitioner filed a Reply. Paper 26 (“Pet. Reply”). Patent Owner filed a Sur-Reply. Paper 30 (“PO Sur-Reply”). An oral hearing was held on November 9, 2023. A transcript of the hearing has been entered as Paper 37. (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a). For the reasons explained below, we determine that Petitioner has met its burden of showing by a preponderance of the evidence that claims 1, 2, 13, 14, 19, and 20 are unpatentable.

A. *Real Parties in Interest*

Petitioner states that ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global

IPR2022-01093
Patent 8,620,039 B2

Corporation, and ASSA ABLOY Global Solutions, Inc., are the real parties in interest.¹ Pet. 1. Patent Owner states that CPC Patent Technologies PTY, LTD is the real party in interest. Paper 4, 2.

B. Related Matters

Petitioner indicates that it filed a declaratory judgment against Patent Owner with respect to the '039 patent in *ABLOY AB, et al. v. CPC Patent Technologies Pty Ltd., et al.*, No. 3-22-cv-00694, in the United States District Court for the District of Connecticut. Pet. 1–2. And Petitioner points out that the '039 Patent is asserted against Apple, Inc., in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, No. 3:22-cv-02553, in the United States District Court for the Northern District of California, San Jose Division. *Id.* Petitioner points out that Apple challenged the '039 patent in IPR2022-00600. *Id.* at 2. On October 13, 2023, we entered a Final Written Decision (Paper 22) in IPR2022-00600 finding claims 1, 2, 19, and 20 of the '039 patent invalid for obviousness.

In addition to the proceedings noted by Petitioner, Patent Owner indicates that “the following judicial and/or administrative matters [] may affect, or be affected by, a decision in this proceeding:” *CPC Patent Technologies PTY Ltd. v. HMD Global Oy*, Case No. 6:21-cv-00166 in the United States District Court for the Western District of Texas; IPR2022-00601; IPR2022-00602; IPR2022-01006; IPR2022-01045; IPR2022-01089; and IPR2022-01094. Paper 4, 2–3.

¹ In its Declaratory Judgment Complaint against Patent Owner, Petitioner also refers to ASSA ABLOY Global Solutions, Inc., as “ASSA ABLOY Global Solutions, Inc. (‘Hospitality’).” Ex. 2007, 2.

C. *The '039 Patent (Ex. 1001)*

The '039 patent, titled “Card Device Security Using Biometrics,” relates to a biometric card pointer (BCP) system intended to more efficiently and securely permit a user to store biometric information during a user enrollment phase, and in future verification processes permits the user access their account using an identification (ID) card and biometric information such as a fingerprint. Ex. 1001, code (54), 2:51–3:11.

The '039 patent explains that in the enrollment phase “[t]he card user’s biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase).” *Id.* at 2:62–64. The '039 patent explains further that “[t]he biometric signature is stored at a memory address defined by the (‘unique’) card information on the user’s card as read by the card reader of the verification station.” *Id.* at 2:64–67. Following the enrollment phase, the '039 patent describes that

[a]ll future uses (referred to as uses in the verification phase) of the particular verification station by someone submitting the aforementioned card requires the card user to submit both the card to the card reader and a biometric signature to the biometric reader, which is verified against the signature stored at the memory address defined by the card information thereby determining if the person submitting the card is authorised to do so.

Id. at 3:4–11.² For both enrollment and future uses, the use of the ID card at a verification station “is identical from the card user’s perspective, requiring

² The words “enrolment,” “authorise,” and “authorisation” are the British spellings of “enrollment,” “authorize,” and “authorization.” *See, e.g.*, <https://www.merriam-webster.com/dictionary/authorisation>, last visited Jan.

IPR2022-01093
Patent 8,620,039 B2

merely input of the card to the card reader, and provision of the biometric signature ([e.g.] thumb print or retinal scan etc.) to the biometric reader.” *Id.* at 3:12–15.

Figure 4 of the '039 patent is reproduced below.

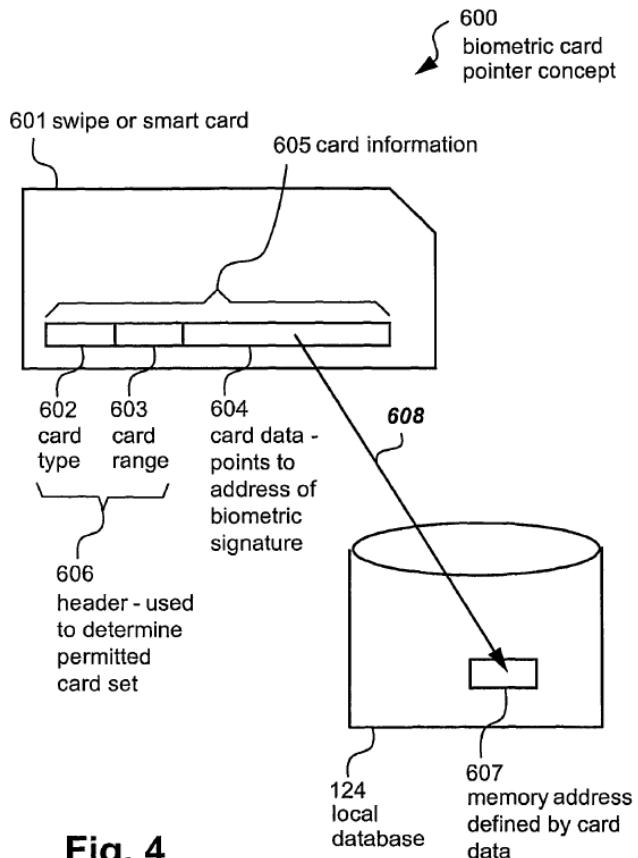


Fig. 4

Figure 4, of the '039 patent, above, illustrates swipe or smart card 601 including card information 605 encompassing fields for card type 602, card range 603, and card data 604. The '039 patent describes that “the card data 604 acts as the memory reference which points, as depicted by an arrow 608,

5, 2023. We will use the American English spelling of these words except where quoted from the '039 patent.

IPR2022-01093
Patent 8,620,039 B2

to a particular memory location at an address 607 in the local database 124.” *Id.* at 7:31–35. Information 605 can be encoded on a magnetic strip on the card, for example. *Id.* at 7:28–29. The ’039 patent explains that for a specific user “[i]n an initial enrolment phase, . . . [t]he card data 604 defines the location 607 in the memory 124 where their unique biometric signature is stored.” *Id.* at 7:43–49. And, the ’039 patent explains further that “in later verification phases, . . . [t]his signature is compared to the signature stored at the memory location 607 in the memory 124, the memory location 607 being defined by the card data 604 read from their card 601 by the card reader 112.” *Id.* at 7:50–56.

Figures 6 and 7, reproduced below, depict the differences between verification process 205 shown in Figure 6, and enrollment process 207 shown in Figure 7.

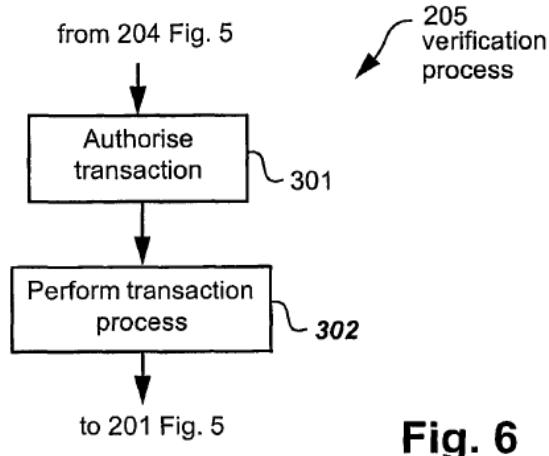


Fig. 6

Figure 6 illustrates verification process 205, which occurs after the enrollment process, illustrated below in Figure 7.

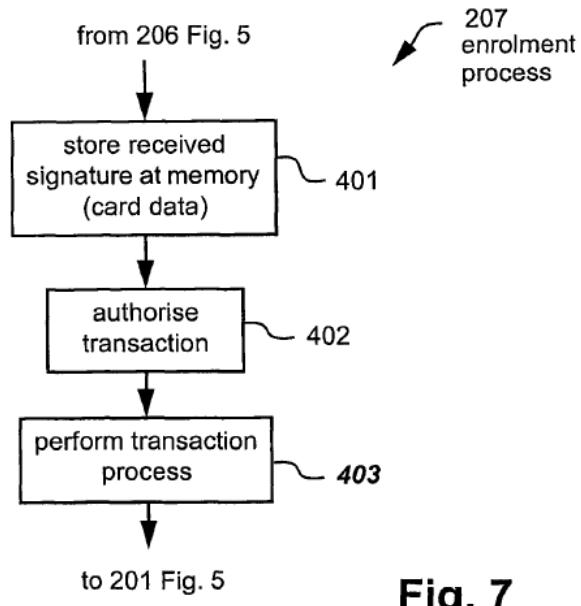
**Fig. 7**

Figure 7 of the '039 patent illustrates enrollment process 207 where the system at “step 401 stores the biometric signature received by the step 203 in the memory 124 at a memory address defined by the card data 604.” *Id.* at 9:64–66 (referring to elements 203 and 124 described in Figure 5). Figure 6 illustrates that verification process 205

is entered from the step 204 in FIG. 5, after which a step 301 authorises the transaction. This authorisation step 301 indicates that the biometric signal received by the biometric reader 102 in the step 203 matches the biometric signature previously stored in the local database 124 by a previous enrolment process 207.

Id. at 9:43–48. Then, “step 204 reads the contents stored at a single memory address defined by the card data 604 and checks these contents against the biometric signature received in the step 203.” *Id.* at 8:34–37.

A difference between verification process 205 and enrollment process 207 is that the enrollment process includes step 401, which *stores* the biometric signature “at a memory address defined by the card data 604,” whereas in verification process 205 “step 204 *reads* the contents stored at a

IPR2022-01093
Patent 8,620,039 B2

single memory address defined by the card data 604” and compares the stored biometric signature with the input biometric signature. *Id.* at 9:65–66, 8:24–26.

D. Illustrative Claim

Claims 1 and 19 are independent. Each of claims 2 and 20 depends, respectively, from independent claims 1 and 19. Claim 1, a method claim, including disputed limitations highlighted in italics, illustrates the claimed subject matter and is reproduced below:

1. 1[P] A method of enrolling in a biometric card pointer system, the method comprising the steps of:
 - 1[A] receiving card information;
 - 1[B] receiving the biometric signature;
 - 1[C] *defining, dependent upon the received card information, a memory location in a local memory external to the card;*
 - 1[D] determining if the defined memory location is unoccupied; and
 - 1[E] storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Ex. 1001, 12:29–38.³ Limitations 1[A]–1[E] are similarly recited in independent claim 13 as an apparatus claim for “[a] biometric card pointer enrolment system,” and also in independent claim 19 in the context of “a processor to execute a method of enrolling in a biometric card pointer system.” *Id.* at 13:67–14:9, 15:25–16:11.

³ We adopt and have applied Petitioner’s alphanumeric designations for the elements of the challenged claims. *See, e.g.*, Pet. 17–37.

IPR2022-01093
Patent 8,620,039 B2

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1, 2, 13, 14, 19, and 20 would have been unpatentable based on the following grounds:

Ground	Claim(s) Challenged	35 U.S.C. § ⁴	Reference(s)/Basis
1	1, 2, 13, 14, 19, 20	103(a)	Hsu, ⁵ Sanford, ⁶
2	1, 2, 13, 14, 19, 20	103(a)	Hsu, Sanford, Tsukamura ⁷

Petitioner relies on the testimony of Stuart Lipoff. Ex 1006 ¶¶ 1–138. Patent Owner presents the testimony of Samuel Russ, Ph.D. Ex. 2039 ¶¶ 1–72.

II. ANALYSIS

A. Legal Standards

A patent claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. 35 U.S.C. § 103; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). “[W]hen a patent claims a structure already known in

⁴ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 296–07 (2011), took effect on September 16, 2011. The changes to 35 U.S.C. §§ 102 and 103 in the AIA do not apply to any patent application filed before March 16, 2013. Because the application for the patent at issue in this proceeding has an effective filing date before March 16, 2013, we refer to the pre-AIA version of the statute.

⁵ Ex. 1003, European Patent Appl'n No. EP 0924655 A2 (pub. June 23, 1999).

⁶ Ex. 1004, PCT Appl'n No. PCT/US03/07238 (pub. Sept. 18, 2003).

⁷ Ex. 1005, US Patent No. 6,963,660 B1 (Nov. 8, 2005).

IPR2022-01093
Patent 8,620,039 B2

the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result.” *KSR*, 550 U.S. at 416 (citing *United States v. Adams*, 383 U.S. 39, 50–51 (1966)). The question of obviousness is resolved based on underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Factors pertinent to a determination of the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology, and (6) educational level of workers active in the field. *Env't'l. Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381–82 (Fed. Cir. 1983)). Not all such factors may be present in every case, and one or more of these or other factors may predominate in a particular case. *Id.* Moreover, these factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. Ltd, Inc. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007).

In determining a level of ordinary skill, we also may look to the prior art, which may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Additionally, the Supreme Court informs us that “[a] person of ordinary skill is also a person of ordinary creativity, not an automaton.” *KSR*, 550 U.S. at 421.

IPR2022-01093
Patent 8,620,039 B2

Petitioner proposes that a person of ordinary skill in the art at the time of the '039 patent "would have had at least an undergraduate degree in electrical engineering, or equivalent education, and at least two years of work experience in the field of security and access-control." Pet. 10–11 (citing Ex. 1006 ¶ 26).

Patent Owner offers the level of ordinary skill we adopted in IPR2022-00600 which is that a person of ordinary skill in the art at the time of the '039 Patent

would have had at least a bachelor's degree in computer engineering, computer science, electrical engineering, or a related field, with at least one year of experience in the field of human-machine interfaces and device access security. Additional education or experience might substitute for the above requirements.

See IPR2022-00600, Paper 22 at 12 (PTAB October 13, 2023) (Final Written Decision).

In this proceeding, Patent Owner's and Petitioner's levels of ordinary skill in the art, in particular education, are not substantively different. Petitioner's proposal requires at least two years of experience in the field of security and access control, compared to one year in Patent Owner's case. We maintain our determination of the level of ordinary skill in the art from IPR2022-00600 including at least one year of experience as Patent Owner urges. On this record, Patent Owner's proposed level of ordinary skill in the art is consistent with our review and understanding of the technology and descriptions in the '039 patent and the asserted prior art references.

Okajima, 261 F.3d at 1355. Indeed, the difference between one and two years of experience in the field is fairly minimal considering that neither party asserts that it is necessary to have a significant amount of experience,

IPR2022-01093
Patent 8,620,039 B2

e.g., 5–10 years in the field. For consistency we rely on the same level of ordinary skill in the art that we determined in IPR2022-00600.

C. *Claim Construction*

We interpret a claim “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b) (2020). Under this standard, we construe the claim “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.* Furthermore, we expressly construe the claims only to the extent necessary. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

1. “*A method of enrolling*”

Patent Owner argues that the independent claims are specifically directed to an enrollment process, e.g., “[a] method of enrolling,” recited in the preamble of claim 1, and that the preamble should be considered limiting. PO Resp. 6. Patent Owner argues that “the ‘method of enrolling’ in the preamble of Claim 1 provides antecedent basis for ‘the enrolment method’ in the body of dependent Claim 2.” *Id.* (citing Ex. 1001, 12:29–42). Petitioner disagrees, arguing that “a ‘method of enrolling’ is nothing more than a nonlimiting intended use.” Pet. Reply 13. Petitioner also asserts that this term is “not critical to the issues in dispute” and “[e]ven if the phrase is limiting, Hsu, Sanford, and Tsukamura each disclose an enrollment process.” *Id.* at 14 (citing Pet. 20, 36–37, 78).

Because Petitioner contends that Hsu, Sanford, and Tsukamura each disclose an enrollment process and Patent Owner does not expressly dispute that they do, in this case we need not explicitly determine whether the term is limiting. We can agree that “[a] method of enrollment” provides antecedent basis for at least dependent claim 2 and that the preamble provides context to the recited method step limitations in the body of independent claim 1. *See* Ex. 1001 12: 41–42 (dependent claim 2 referring “to the enrollment method of claim 1”). Apart from considering the limitations of claim 1 within the context of an enrollment process, because the term does not create any particular dispute between the parties that we need to resolve, we need not determine whether it is limiting.

2. “*dependent upon*”

Petitioner indicates that the parties agreed in the district court litigation that “dependent upon,” recited in claim 1 and 19, should be given its plain and ordinary meaning, “defined as ‘contingent on or determined by.’” Pet. 16 (citing Ex. 1013, 2). Patent Owner agrees, adding that “a memory location in a local memory which merely corresponds to, *but is not contingent upon or determined by*, the received card information is not ‘dependent upon’ the received card information.” PO Resp. 10 (citing Ex. 2039 ¶ 33). Patent Owner points out that Petitioner asserts the meaning of “dependent upon” is not material to patentability. *Id.* Patent Owner contends, however, that “because ‘dependent upon’ is integral to the ‘defining, *dependent upon* the received card information, a memory location in a local memory external to the card’, its meaning must be considered when analyzing the entire claim term.” *Id.*

We agree that for purposes of understanding claim 1, we should consider the plain and ordinary meaning of “dependent upon,” so that limitation 1[c] is understood as follows:

[1c] defining, [contingent upon or determined by] the received card information, a memory location in a local memory external to the card;

Accordingly, in this proceeding, we will consistently apply the plain and ordinary meaning of “dependent upon” which is “contingent upon or determined by.”

3. *“defining, dependent upon the received card information, a memory location in a local memory external to the card”*

Patent Owner argues that “the proper construction of this entire clause is: ‘the system sets or establishes a memory location in a local memory external to the card, said location being contingent upon or determined by the received card information.’” PO Resp. 11. Patent Owner asserts that a person of ordinary skill in the art “would interpret the word ‘defining,’ especially in the context of enrollment, to mean ‘setting’ or ‘establishing.’” *Id.* at 12.

Petitioner proposes alternative constructions, first that “defining” means that “a memory location is somehow determined from (or is dependent on) the card information.” Pet. 11. Second, that “defining” means “a memory location is specified by the card information itself.” Petitioner contends that the second construction is most consistent with the specification of the ’039 patent specification. *Id.* at 12. According to Petitioner, and considering that the ’039 describes “a biometric card pointer system,” a person of ordinary skill in the art “would have understood that the user’s card information itself specifies the physical memory address (such as

IPR2022-01093
Patent 8,620,039 B2

by acting as a pointer) for the user’s biometric signature.” *Id.* at 13 (citing Ex. 1006 ¶ 47).

Consistent with our prior decision in IPR2022-00600, we determine, also in this proceeding, that Patent Owner’s construction is sufficiently accurate. *See Apple, Inc. v. CPC Patent Technologies, Ltd.*, IPR2022-00600, Paper 22, 29–39 (Final Written Decision); *see also NTP Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1293 (Fed. Cir. 2005) (noting that, when construing claims in patents that derive from the same parent application and share common terms, “we must interpret the claims consistently across all asserted patents”). In IPR2033-00600, we explained that

[c]onsidering the abstract and the specification of the ’039 patent, what “defining, dependent upon . . .” means as a whole, in the context of claim 1 and “a method of enrolling,” is that during an *enrollment* process, the claimed “biometric signature,” e.g., a fingerprint, is not yet stored in the memory and no memory location or address has been “set” or “established” for the fingerprint. When the fingerprint, and then the card, is provided to the system during enrollment, the card information provides data that establishes *where*, e.g., at what memory location or address, the system will *store* the fingerprint data.⁸

IPR2022-00600, Paper 22, 30. We also explained that “[i]mportantly . . . we do not understand that ‘defining . . . a memory location,’ or Patent Owner’s alternative wording, ‘establishing’ or ‘setting,’ means ‘[creating] . . . a memory location in a local memory.’” *Id.* at 32. We explained further that

⁸ We use the terms “memory location” and “memory address” interchangeably because, in terms of computer memory, an “address” is well-understood as “[a] number specifying a location in memory where data is stored.” MICROSOFT COMPUTER DICTIONARY, 5th Ed. (2002) Microsoft Press.

IPR2022-01093
Patent 8,620,039 B2

“[w]hile we might agree that ‘the memory location cannot [already be defined],’ . . . we do not agree that it ‘cannot already exist.’” *Id.* at 33.

During the oral hearing in this proceeding, Patent Owner’s counsel argued that “Patent Owner in this case has not argued that defining means creating.” Tr. 31:3–4. Patent Owner’s counsel argued further, “[a]ll we’re saying that Claim 1 requires is that when a user swipes their card, that is the information that is on the card, not – in that moment in time, not something else in the system, but the information on the card that directs the system where to store that particular user’s fingerprint or other biometric data.” *Id.* at 31:7–11.

Considering Patent Owner’s arguments and asserted claim construction with respect to the phrase “defining, dependent upon” and limitation 1[C] as a whole, we maintain the claim construction given in IPR2022-00600 for the reasons given in the Final Written Decision. IPR2022-00600, Paper 22, 30. We understand that during an enrollment process the claimed “biometric signature,” e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been “defined,” as in “set” or “established,” in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint are received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data.

4. “*unoccupied*”

In our Institution Decision, as argued by Petitioner and based on the express written description of the ’039 patent, we determined that “*unoccupied*” means “a memory location that has not been used in the enrollment process for a user, or the information stored at the memory

IPR2022-01093
Patent 8,620,039 B2

location has been deleted.” Inst. Dec. 38–39; *see also* Ex. 1001, 9:29–33 (“The term ‘occupied’ in this context means that the memory location in question has been used in the enrolment process for a user, and that the information stored at the memory location in question has not been deleted by a BCP system administrator.”). Patent Owner does not dispute this construction. PO Resp. 14.

Although patentability on the claims at issue in this case does not turn on the construction of this term, we nevertheless maintain our construction from our Institution Decision that “unoccupied” means “a memory location that has not been used in the enrollment process for a user, or the information stored at the memory location has been deleted.” Inst. Dec. 38–39.

5. *Other claim terms agreed upon and construed by the District Court*

The parties indicate that the following terms have been construed by the District Court:

“*biometric card pointer system*” – Nonlimiting preamble term with no patentable weight;

“*biometric card pointer enrollment system*” – Nonlimiting preamble term with no patentable weight;

“*biometric signature*” – Plain and ordinary meaning.

Pet. 16 (citing Ex. 1012, 1); PO Resp. 15 (citing Ex. 1012, 2).

Considering these constructions and that our analysis does not turn on any particular claim construction for these terms, and because these constructions are not in dispute, we need not determine any specific claim construction for these terms in this proceeding.

6. *Means-plus-function terms*

In our Institution Decision we accepted Petitioner's proposed constructions for the several "means for" and "code for" limitations recited in claims 13, 14, 19, and 20. *See* Inst. Dec. 43 (The Board explaining that "we find Petitioner's proposed constructions of these term under 35 U.S.C. § 112(6) consistent with the record in this case."). These constructions are also consistent with the District Court proceeding. Inst. Dec. 39–43; *see also* Ex. 1012, 1–4. For its part, Patent Owner states that it "takes no position on these proposed constructions as they are not material to the alleged grounds for unpatentability asserted in the Petition." PO Resp. 15.

Based on our review of the complete trial record and because patentability on the claims at issue in this case does not turn on construction of the relative structures and functions of these means-plus-function terms, and because they are not in dispute, we maintain the constructions from our Institution Decision including that "code for" is an equivalent recitation for "means for." Inst. Dec. 39–43.

D. *Ground 1: Claims 1, 2, 13, 14, 19 and 20 – Obviousness over Hsu (Ex. 1003) and Sanford (Ex. 1004)*

For the reasons below, and on the complete record before us, Petitioner has shown by a preponderance of the evidence that claims 1, 2, 13, 14, 19, and 20 would have been obvious over Hsu and Sanford.

1. *Hsu (Ex. 1003)*

Titled "Controlled Access to Doors and Machines Using Fingerprint Matching," Hsu describes "[a] system and related method for controlling access to building doors or to machines, such as automatic teller machines (ATMs)." Ex. 1003, Abstract, codes (54), (57). Hsu describes using "an account number or employee number, to access a fingerprint database (44)

IPR2022-01093
Patent 8,620,039 B2

and retrieve reference fingerprint data previously stored there during an enrollment procedure.” *Id.*, Abstract. Figure 3 from Hsu, as annotated by Petitioner (Pet. 8), is reproduced below.

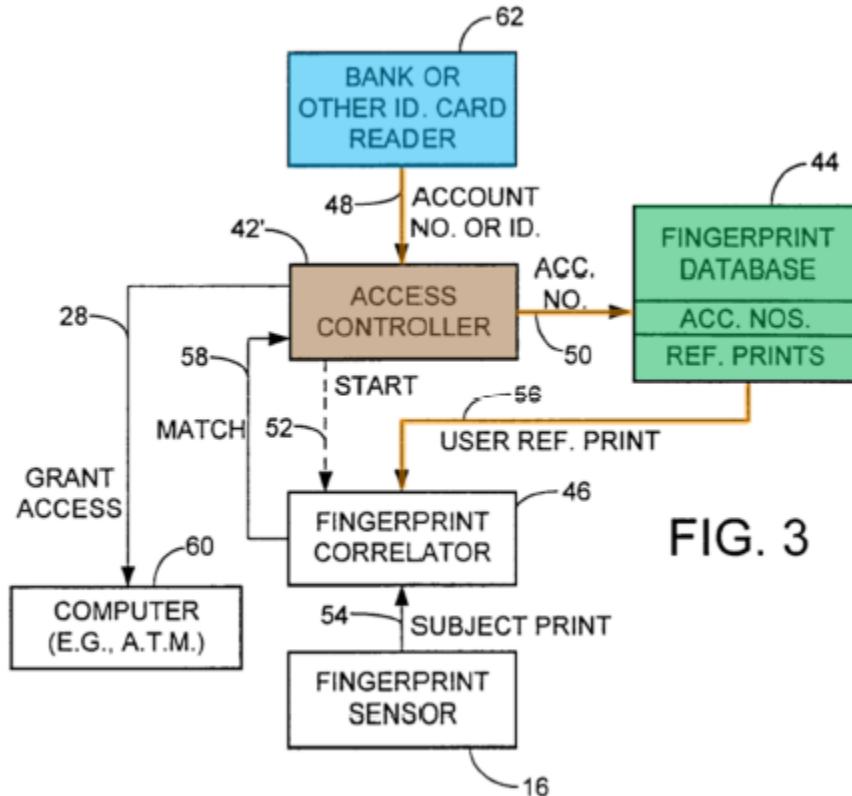


FIG. 3

Hsu’s Figure 3 is a block diagram illustrating card reader 62 (blue) reading “an account number or other type of identification unique to the user, and passes this data to the access controller 42’ [(brown)] over line 48.”

Ex. 1003, 6:10–12. Based on the user’s unique identification, access controller 42’ communicates with finger print database 44 (green) “to access the fingerprint database 44 and obtain a user reference fingerprint on line 56 from the database.” *Id.* at 6:14–16. Hsu explains that

[t]he controller 42’ also sends a “start” signal on line 58 to the fingerprint correlator 46, which compares the reference fingerprint with a subject fingerprint image supplied from the sensor 16 over line 54. If the correlator 46 finds a match, the correlator sends a signal over line 58 to the access controller 42’,

which transmits an appropriate signal to the computer 60 on line 28, indicating that access has been granted.

Id. at 6:16–24.

Hsu also describes an enrollment process shown in Figure 4 and reproduced below.

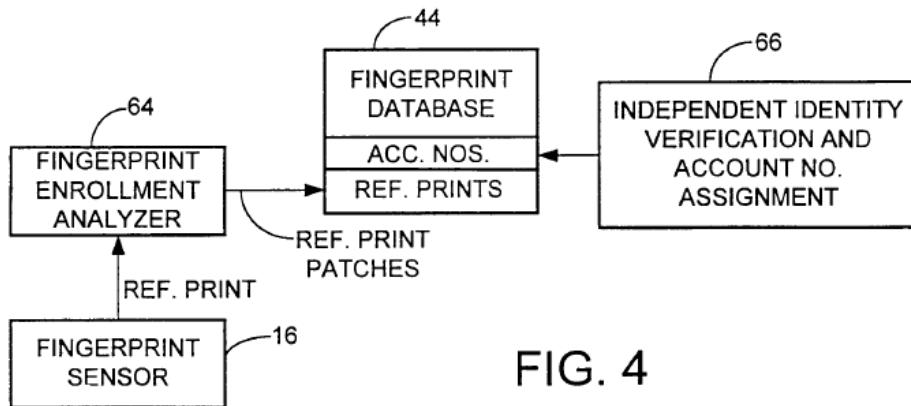


FIG. 4

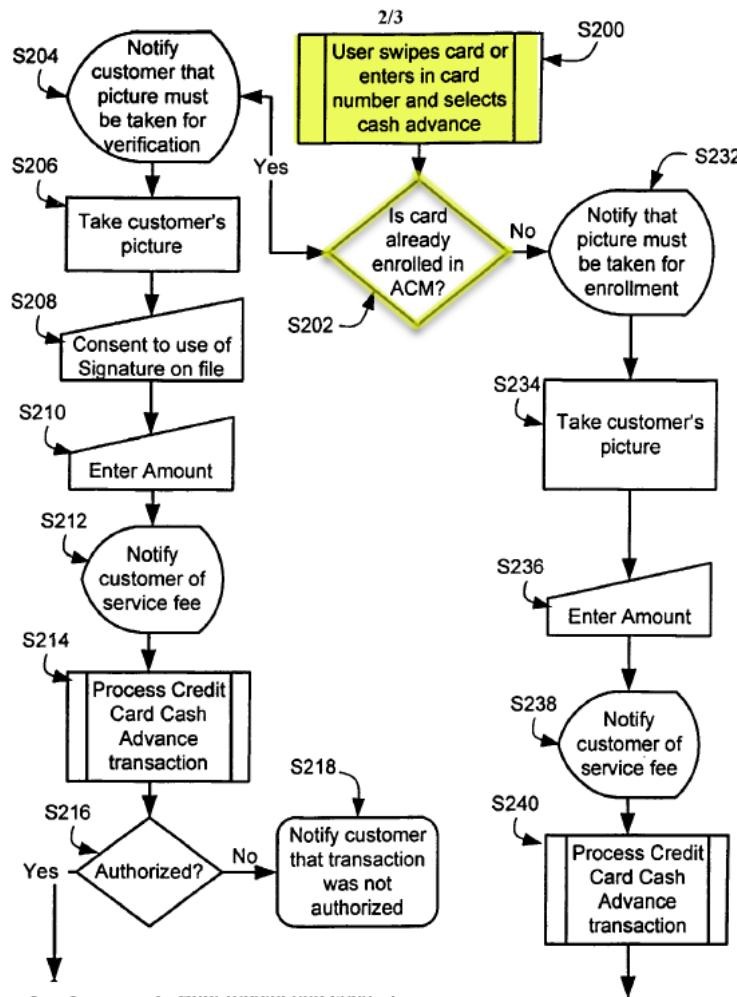
Hsu's Figure 4 illustrates a block diagram showing that a user's fingerprint is obtained by fingerprint sensor 16 and passes through fingerprint enrollment analyzer 64 before being stored in fingerprint database 44. *Id.* at 7:51–8:23. Hsu explains that, along with providing a fingerprint during enrollment, “[a]t the same time, the user's identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the user also presents an account number, employee number or similar identity number.” *Id.*

2. *Sanford (Ex. 1004)*

Sanford is titled “Credit Card Transaction without using a Pin with Automated Cashier Machine” and describes “[a]n automated cashier machine (ACM) is provided that offers a secure and convenient way for users to access cash from their card without using a PIN.” Ex. 1004, Abstract, codes (54), (57). Sanford describes that “[b]y verifying a user's image using facial biometrics, transactions may be conducted without using

IPR2022-01093
Patent 8,620,039 B2

a pin.” *Id.* ¶ 7. Sanford explains further that “[o]ther methods of verification known in the art may also be used, such as iris, voice signature, and fingerprint technology.” *Id.* ¶ 20. The relevant part of Sanford’s Figure 2, as annotated by the Board, is reproduced below.



Sanford’s figure 2 is a block diagram illustrating a method for performing a PIN-less credit card transaction using an ACM (automated cashier machine). *Id.* ¶ 24. After swiping a user’s card at step 200, the system determines whether the user’s card information is already stored, i.e., enrolled, and “the ACM 12 determines if the credit card account number of the user is enrolled to use the PIN-less credit card system.” *Id.* In determining if the user is enrolled, “ACM 12 may communicate with ACM computer system 18 to

IPR2022-01093
Patent 8,620,039 B2

look up the user's credit card number." *Id.* ¶ 25. At step 202, highlighted yellow above, ACM 12 determines an enrollment course of action; if the card is not enrolled, moving to step 232, or, if the card is already enrolled, conducting a verification course of action via step 204. *Id.*

3. Independent Claim 1

We consider initially the elements of claim 1.

a) Petitioner's Arguments

(1) Preamble – 1[P] "A method of enrolling in a biometric card pointer system"

To the extent the preamble could be considered limiting, Petitioner argues that Hsu teaches "a biometric card pointer system" where "access control unit 14 includes an access controller (42 or 42') that "uses the account number [or user number] . . . to access the fingerprint database 44 [green] and obtain a user reference fingerprint." Pet. 19 (citing Ex. 1006 ¶¶ 20, 24). With respect to "enrolling," Petitioner contends that Hsu's Figure 4 "discloses 'a method of enrolling' in its biometric card pointer system. Specifically, 'FIG. 4 is a block diagram showing a fingerprint enrollment process as used in FIG[. 3.]'" *Id.* at 20 (quoting Ex. 1003 ¶ 14). Hsu's Figure 4, as annotated by Petitioner (*id.* at 20), is reproduced below.

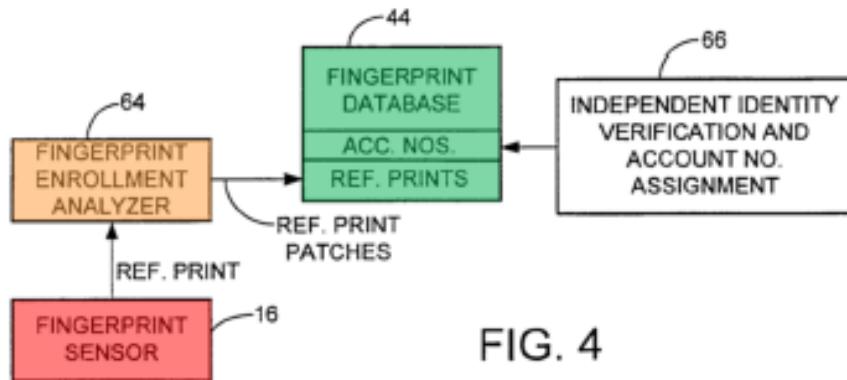


FIG. 4

IPR2022-01093
Patent 8,620,039 B2

Figure 4 is a block diagram illustrating “a fingerprint enrollment process as used in either of the systems of FIGS. 2 and 3.” Ex. 1003 ¶ 14. Mr. Lipoff testifies that considering Hsu’s Figure 4 “[a]s shown, ‘[t]he account number is stored in the database 44 [green] in association with the user’s fingerprint image data.’ Once a user is enrolled, he or she may use his or her card to access his or her reference fingerprint for verification purposes.” Ex. 1006 ¶ 73 (quoting Ex. 1003 ¶ 24).

(2) *Limitation 1[A] – “receiving card information”*

Petitioner points to Hsu’s Figure 3 and argues that a person of ordinary skill in the art “would have understood that Hsu’s received ‘account number’ is the claimed ‘card information.’” Pet. 23 (citing Ex. 1006 ¶ 78). Petitioner argues that “Hsu’s enrollment process also includes ‘receiving card information.’ Hsu includes various disclosures of ‘reading data from a card reader,’ which confirm that the card reader (or its equivalent, a polling transceiver) in the access controller is receiving card information.” *Id.* (citing Ex. 1003 ¶ 9). Mr. Lipoff testifies that based on Hsu’s “various disclosures of ‘reading data from a card reader,’ . . . a person of ordinary skill in the art “would have understood that regardless of the type of card used, Hsu’s enrollment process includes receiving card information (e.g., account number or employee number).” Ex. 1006 ¶¶ 79–80 (citing Ex. 1009 ¶¶ 9, 26).

(3) *Limitation 1[B] – “receiving the biometric signature”*

Petitioner argues that as shown in Hsu’s Figure 1, “the access control unit includes a ‘fingerprint sensor 16’ (red) for ‘scan[ning] the user’s

fingerprint.’’’ Pet. 26 (citing Ex. 1003 ¶¶ 20–21, 24). Hsu’s Figure 1 as annotated by Petitioner (*id.* at 27) is reproduced below.

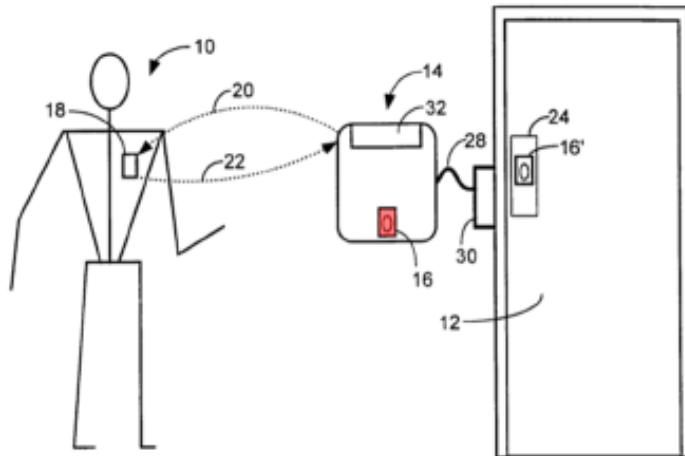


FIG. 1

Hsu’s Figure 1 depicts access controller 14 having fingerprint sensor 16 (highlighted red) for receiving a fingerprint from user 10. *See* Ex. 1003 ¶ 17 (“When the user 10 reaches the door, he or she places a finger on the fingerprint sensor 16.”).

(4) *Limitation 1[C] – “defining, dependent upon the received card information, a memory location in a local memory external to the card”*

Petitioner argues specifically that Hsu’s Figure 1 “discloses ‘a local memory external to the card.’ As shown in Figure 1, the ‘access control unit 14’ (yellow) is external to the ‘identification badge 18 [card]’ (pink).” Pet. 28. Hsu’s Figure 1 as annotated by Petitioner (*id.* at 28) is reproduced below.

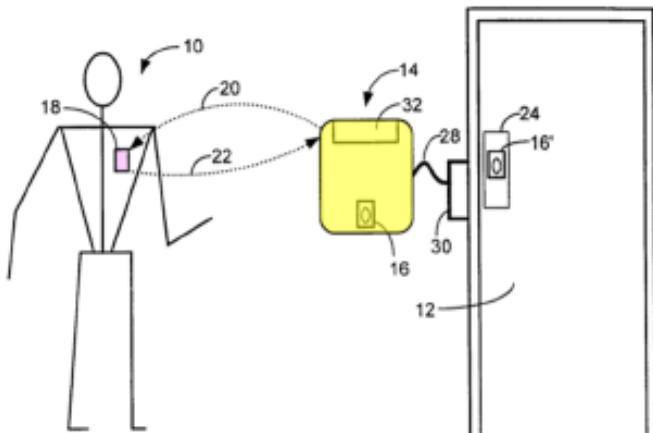


FIG. 1

Hsu's Figure 1 depicts access controller 14 (highlighted yellow) which is separate, i.e., external to the card or ID badge 18 (highlighted pink) worn by user 10. *See Ex. 1003 ¶ 20* (access controller 14 includes "fingerprint database 44, and a fingerprint correlator 46"). Mr. Lipoff testifies that a person of ordinary skill in the art "would also have understood that a database is stored in a memory. Thus, in my opinion, the 'fingerprint database (44)' in Figure 2 of Hsu discloses 'a local memory external to the card.'" Ex. 1006 ¶ 90.

Petitioner argues with respect to the phrase "defining dependent upon the received card information, a memory location . . ." that Hsu specifically discloses "[t]he database is basically a table that associates each user number with a stored fingerprint image, or with selected distinctive attributes or features of the user's fingerprint image." Pet. 31 (quoting Ex. 1003 ¶ 20). Hsu's Figure 4, as annotated by Petitioner (*id.* at 20), is reproduced below.

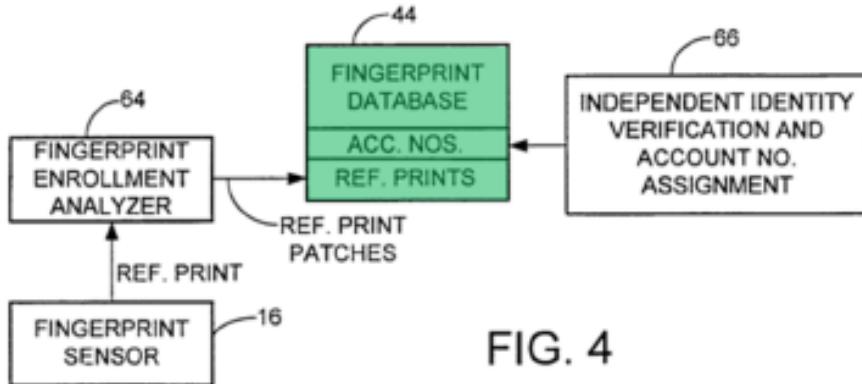


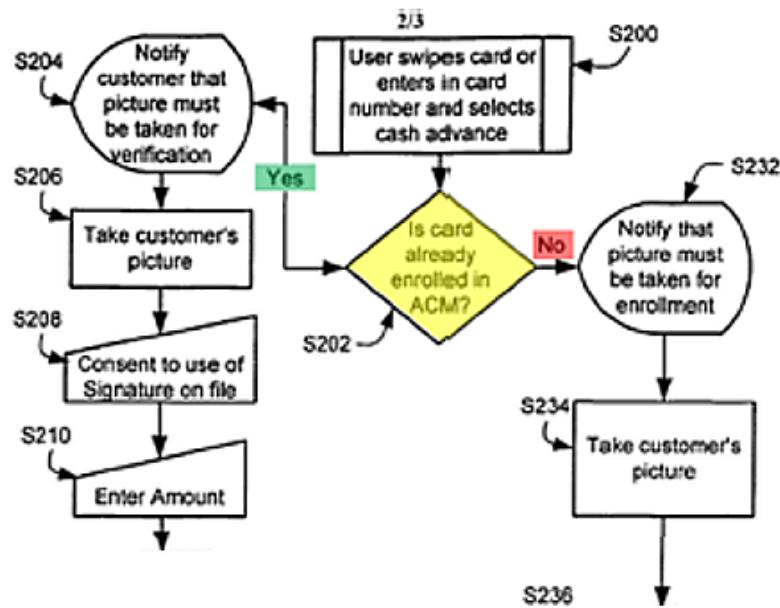
FIG. 4

Hsu's Figure 4 is a block diagram of an enrollment process illustrating fingerprint database 44 (highlighted green) including reference prints and related account number for each user or employee. Ex. 1003 ¶ 26.

Mr. Lipoff testifies that a person of ordinary skill in the art "would have understood that, given a user [account] number, Hsu's system easily determines from fingerprint database 44 the specific memory location for storing the associated fingerprint." Ex. 1006 ¶ 93.

(5) *Limitation 1[D] – “determining if the defined memory location is unoccupied”*

Petitioner argues that Hsu in combination with Sanford renders claim limitation 1[D] obvious. Pet. 32. Petitioner asserts that Hsu discloses the "defined memory location," but does not explicitly discuss determining whether a memory location is occupied or not. *Id.* Petitioner turns to Sanford, arguing that "Sanford discloses in step S202 (yellow) 'determin[ing] if the credit card account number of the user is enrolled to use the PIN-less credit card system.'" *Id.* at 33. Sanford's Figure 2, in relevant part, and as annotated by Petitioner (*id.* at 34), is reproduced below.



Sanford's Figure 2, reproduced in part above, as annotated by Petitioner, is a block diagram illustrating a decision making process at step 202 (highlighted yellow) based on whether a user's card is enrolled (yes, highlighted in green) or not (no, highlighted in red) in the ACM. *See Ex. 1004, Fig. 2.*

With respect to a motivation to combine Hsu and Sanford, which we address in further detail below, Mr. Lipoff testifies that a person of ordinary skill in the art, understanding that Hsu has a database that may include a fingerprint associated with a user or employee number, "would not want to enroll a user who already enrolled." Ex. 1006 ¶ 112 (citing Ex. 1004 ¶ 38). Mr. Lipoff explains that "[r]e-enrollment is usually unnecessary because fingerprints do not change. Re-enrollment also consumes unnecessary system resources, takes time, and is generally undesirable. Therefore, before enrolling a user, it is my opinion that a POSITA would have been motivated to first check whether the user is already enrolled, as disclosed by Sanford." *Id.* Mr. Lipoff testifies further that "checking whether a user is enrolled also

makes the system more user-friendly. If the user is enrolled, the user can seamlessly proceed with biometric verification.” *Id.* ¶ 114.

(6) *Limitation 1[E] – “storing, if the memory location is unoccupied, the biometric signature at the defined memory location”*

Following from limitations 1[C]–[D], Petitioner argues that Hsu in combination with Sanford renders claim limitation 1[E] obvious, because “Sanford discloses that if a user is not enrolled (*i.e.*, if Hsu’s memory location is unoccupied), the user is directed to complete enrollment, which involves storing the user’s biometric information (*e.g.*, picture or fingerprint) in the database.” Pet. 36 (citing Ex. 1004 ¶ 37). Mr. Lipoff testifies that because both Hsu and Sanford disclose an enrollment process for a user, where Sanford teaches checking if a storage location is unoccupied, a person of ordinary skill in the art, would have known to, “*e.g.*, check[] Hsu’s database to see if a user is not yet enrolled per Sanford, and if so, storing], the biometric signature [*e.g.*, user’s fingerprint] at the defined memory location [*e.g.*, at the memory address in Hsu’s database assigned to the user].” Ex. 1006 ¶ 107.

(7) *Analogous Art and Motivation to Combine Hsu and Sanford*

Petitioner’s assertion that Hsu and Sanford are analogous art to the ’039 Patent, and Petitioner’s evidence and arguments as to motivation to combine, are undisputed by Patent Owner. *See generally* Prelim. Resp. For completeness, we address Petitioner’s foundational arguments and evidence as to analogous art and motivation to combine to ensure that Petitioner has met its burden under 35 U.S.C. §§ 312 (a)(3), 316(e).

(a) Analogous Art

Petitioner argues that Hsu and Sanford are analogous prior art with respect to the '039 patent. Pet. 37. Petitioner contends that “[b]oth references (and the '039 Patent) are directed to ways of performing efficient biometric authentication, including using fingerprints.” *Id.* Petitioner argues that “[b]oth references (and the '039 Patent) teach authenticating a user by comparing a fingerprint captured by a sensor to a stored fingerprint.” *Id.* (citing Ex. 1003, Abstract; Ex. 1004, Abstract).

As to analogous art, we consider two criteria when evaluating whether prior art is analogous: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the inventor’s endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.

In re Clay, 966 F.2d 656, 658–59 (Fed. Cir. 1992).

The '039 patent is directed broadly to “security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs.” Ex. 1001, 1:14–16. More specifically, the '039 patent explains that its disclosure addresses “problems relating to secure access and/or secure processes, by automatically storing a card user’s biometric signature in a local memory in a verification station comprising a card reader, [and] a biometric signature reader.” *Id.* at 2:53–57. Based on this, a reasonable field of endeavor involves enrollment and user verification systems including card devices and biometric signatures.

As Petitioner points out, both Hsu and Sanford expressly disclose enrollment and biometric user verification systems that compare a user fingerprint to a stored fingerprint for identity verification purposes.

See, e.g., Ex. 1003 ¶¶ 4, 13, 20, 24, Fig. 3, *see also* Ex. 1004 ¶¶ 4, 8–9, 16,

36. For example, Hsu explains that “FIG. 2 shows the principal components of the access control unit 14 in block diagram form, including an identification polling transceiver 40, a door controller 42, a fingerprint database 44, and a fingerprint correlator 46.” *Id.* at ¶20. Similarly, Sanford describes that in “a secure and convenient way for users to access cash from their card without using a PIN . . . [a]n identifying image of a user is taken and an amount for withdraw is received. If the amount for withdrawal is approved, the ACM verifies the identifying image of the user to an image of the user in a profile.” Ex. 1004 ¶6. Also, Sanford states that “[o]ther methods of verification known in the art may also be used, such as iris, voice signature, and fingerprint technology.” *Id.* ¶20.

On the complete record now before us, we are persuaded that Hsu and Sanford are analogous art to the ’039 patent as they are directed to the same field of endeavor, which is enrollment and user verification systems including card devices and biometric signatures.

(b) Motivation to Combine

With respect to a motivation to combine, Petitioner argues that although Hsu does not expressly disclose checking if the memory location in Hsu’s database assigned to the user is unoccupied “this would be obvious to a POSITA.” Pet. 32. To this end, Petitioner argues that Sanford describes an algorithm including a “check of whether a user is enrolled into Hsu’s system.” *Id.* at 37 (citing Ex. 1006 ¶ 108). Petitioner points out that Hsu describes an embodiment “where the user already has an account/user/employee number but has not yet enrolled their fingerprint.” *Id.* at 26 (citing Ex. 1006 ¶ 110). Petitioner argues that “[i]n this context, a POSITA would have been motivated to implement Sanford’s check to determine whether a

IPR2022-01093
Patent 8,620,039 B2

user (e.g., with a user/account number) is enrolled in Hsu’s system.” *Id.* (citing Ex. 1006 ¶ 111).

In support, Petitioner’s declarant, Mr. Lipoff, testifies that a person of ordinary skill in the art would have implemented Sanford’s check to determine whether a user is enrolled in Hsu’s system, for several reasons. Ex. 1006 ¶¶ 111–114. First, Mr. Lipoff explains, “in most instances, a POSITA would not want to enroll a user who already enrolled” because “[r]e-enrollment also consumes unnecessary system resources, takes time, and is generally undesirable.” *Id.* ¶ 112. Second, Mr. Lipoff explains that “checking whether a user is enrolled helps prevent fraud whereby an unauthorized user is able to overwrite the fingerprint of an authorized user by using the authorized user’s user number or account number.” *Id.* ¶ 113. Also, Mr. Lipoff testifies that “checking whether a user is enrolled also makes the system more user-friendly. If the user is enrolled, the user can seamlessly proceed with biometric verification.” *Id.* ¶ 114.

On the complete record now before us, we find persuasive Petitioner’s explanations for a motivation to combine Hsu and Sanford. Sanford, as Mr. Lipoff testifies persuasively, describes *how* a person of ordinary skill in the art would construct a system to check to see if a user is enrolled in a biometric identity verification system before determining a further course of action. *Id.* ¶¶ 98–100. In addition, Mr. Lipoff provides several reasons *why* a person of ordinary skill in the art would have looked to Sanford for “the simple and straightforward way to determine whether such user has been enrolled [and] to check if the user’s data is already stored in Hsu’s database.” *Id.* ¶ 115; *see also* KSR, 550 U.S. at 420 (explaining that “any need or problem known in the field of endeavor at the time of invention and

IPR2022-01093
Patent 8,620,039 B2

addressed by the patent can provide a reason for combining the elements in the manner claimed”).

b) Patent Owner’s Arguments

Patent Owner focuses its arguments on limitation 1[C], arguing that “Hsu is devoid of any teaching or suggestion that the user’s card information sets or establishes (*i.e.*, defines) the memory location for the user’s fingerprint data during enrollment.” PO Resp. 16 (citing Ex. 2039 ¶46). According to Patent Owner, Hsu does not “set” or “establish” a memory location for the fingerprint data because Hsu mainly describes that “[t]he account number is stored in the database 44 in association with the user’s fingerprint image data.” *Id.* at 17 (quoting Ex. 1003, 7:1–12). Patent Owner’s position is that Hsu doesn’t define any memory location in particular, but “that the user’s fingerprint data and account number are presented *at the same time* and are then stored in the database *in association with* each other.” *Id.* at 18 (citing Ex. 2039 ¶49). In other words, Patent Owner’s argument is that, unlike the claimed method, Hsu’s card information does not provide data that sets or establishes *where*, *i.e.*, at what memory location or address, the system will *store* the fingerprint data.

c) Analysis

Hsu expressly describes an enrollment process for a user including fingerprint database 44 and describes that “the fingerprint database 44 contains reference fingerprint image data for each user, employee, or customer using the system, and that the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers.” Ex. 1003 ¶26. Hsu’s Figure 4, illustrating the enrollment process, as annotated by Petitioner (Pet. 20), is reproduced below.

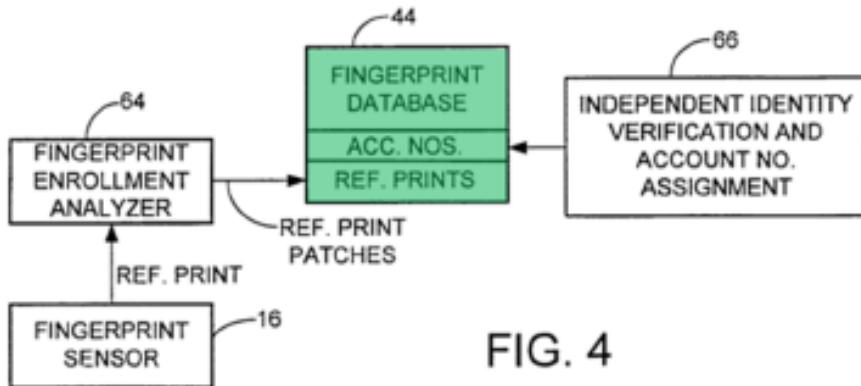


FIG. 4

Hsu's Figure 4 is a block diagram showing an enrollment process illustrating fingerprint database 44 (highlighted green) including reference prints and related account number for each user or employee. Ex. 1003 ¶26.

Based on the description and Figure 4, Hsu tells us a location, that is *where*, i.e., in fingerprint database 44, the fingerprint is to be stored during enrollment. Hsu explains that in fingerprint database 44, "fingerprint data are associated with corresponding user numbers, or employee or customer account numbers." *Id.* Accordingly, we understand from this description that the user's fingerprint is stored in relation to, i.e., "associated with," the user's employee account number, for example. Still, a key question is *how* is the fingerprint data stored during enrollment, because, consistent with our claim construction, the card information must "set" or "establish" where the fingerprint data is to be stored. This question is also answered by Hsu. Hsu explains that when a user presents a fingerprint during enrollment, "[a]t the same time, the user's identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the user also presents an account number, employee number or similar identity number." *Id.* In this way, Hsu describes presenting identification data apart from biometric data, and includes presenting, for example, an employee

IPR2022-01093
Patent 8,620,039 B2

identification card or badge, including the user's employee number. *See Ex. 1003 ¶ 11* (Hsu describing that "the identification medium carried by each user includes a machine-readable card, and the step of reading data from an identification medium includes reading data from a card reader in which the machine-readable card is placed by the user"). Understanding that during enrollment Hsu stores the user's fingerprint data "associated with" a user's employee number on the card, we further understand that the identification information, e.g., employee number, on the identification card defines, sets, or establishes *where* the fingerprint is stored; that is, the user's fingerprint data is stored with the database record corresponding to the relevant employee number.

Given this, we conclude that Patent Owner's position that Hsu does not disclose a memory location "defined by," "set," or "established" by card information is not accurate. Patent Owner's argument mainly contrasts the terms "associated with," as described in Hsu, with our claim construction that "defined by," means "set" or "established." We agree that these are different words, but an ordinary meaning of "associated" is "related, connected, or combined together." MERRIAM WEBSTER ONLINE DICTIONARY, <https://www.merriam-webster.com/dictionary/associated> (last visited Jan. 9, 2024) (Ex. 3001). Considering common database structures and functions, we are persuaded that Hsu, by "associating" a user's fingerprint data with a database record corresponding to a particular employee, concomitantly discloses "defining," "setting," or "establishing" a memory location for the fingerprint data in relation to the employee account number. Consistent with our understanding of Hsu's disclosure, Mr. Lipoff testifies persuasively that in Hsu "[t]he 'fingerprint image, or [] selected distinctive attributes or features of the user's fingerprint image' are not

IPR2022-01093
Patent 8,620,039 B2

stored at *any* memory location in the database—rather, it is stored at a memory location associated with the specific user/employee number received from a card.” Ex. 1006 ¶ 93 (citing Ex. 1003 ¶ 26).

Patent Owner’s counsel made clear, during oral argument, its position that “there’s no discussion at all in Hsu that the ID number/card information in enrollment for purposes of storing the signature, stores [fingerprint data] at a specified location – by location specifically specified by the card data.” Ex. 3001 42:21–23. But we do not agree with this position. As discussed above, Hsu describes that fingerprint data is stored associated with the card data, e.g., an account or employee number. Ex. 1003 ¶ 26 (Hsu describing that “the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers.”). Consistent with our claim construction, the “association” is the *where*. In other words, we understand that Hsu’s associating the fingerprint data with the personal data record in fingerprint database 44 defines, sets, or establishes where the fingerprint data is stored. This occurs, as Hsu explains, because during enrollment the user data such as account or employee number is supplied by the user’s card. *Id.* ¶ 11. We do not see it as a significant leap to understand that in Hsu the user’s personal data record is the location with which the fingerprint data is associated and stored in fingerprint database 44.

Patent Owner also argues that “[i]n contrast to the claimed method, Hsu teaches that the user’s fingerprint data and account number are presented *at the same time* and are then stored in the database *in association with* each other.” PO Resp. 18 (citing Ex. 2039 ¶ 49). Patent Owner’s declarant, Dr. Russ, similarly testifies that “in Hsu, the fingerprint data and the account number are presented together and are then stored together . . . [t]here is no step in Hsu wherein the account number (or the ‘card

IPR2022-01093
Patent 8,620,039 B2

information') first sets or establishes the memory location." Ex. 2039 ¶ 49. This argument takes advantage of the fact that Hsu does not explicitly state a temporal order for "storing . . . the biometric signature" as recited in claim 1. However, as we explained in our claim construction,

during an enrollment process the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been "defined," as in "set" or "established," in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint is received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data.

Section II.C.3. Similarly, in Hsu, the fingerprint data can only be stored once the system has received data indicative of, for instance, an employee number from a user's identification badge, which thus defines a database record with which the fingerprint data can be "associated."

This all makes sense, logically, because Hsu's fingerprint data are not randomly stored, as Mr. Lipoff explains, "in *any* memory location."

Ex. 1006 ¶ 93. Hsu's fingerprint data cannot be stored until directed to, i.e. "associated with," a certain database address or record, and in Hsu that is a database record containing the user's identification information.

See Ex. 1003, 7:7–12. (Hsu describing that during enrollment "the user also presents an account number, employee number or similar identity number . . . [t]he account number is stored in the database 44 in association with the user's fingerprint image data"). Accordingly, from a temporal standpoint during enrollment, Hsu must also use card information, e.g., an employee number stored on the card, to define, set, or establish a memory location before storing the fingerprint data, wherein the employee number is associated with the fingerprint data. Commensurate with our understanding

IPR2022-01093
Patent 8,620,039 B2

of Hsu's disclosure, we credit Mr. Lipoff's testimony that even though Hsu does not explain exactly "how a new user record is created" during enrollment, a person of ordinary skill in the art would "try using simple known options for creating database records." Ex. 1032 ¶ 33. Mr. Lipoff explains persuasively that "upon a user enrolling, they provide a previously unseen card/user number, [and] the system then creates a new record for the user, including setting/establishing for the first time the memory location for storing the user's fingerprint." *Id.* ¶ 34.

When asked during his deposition to describe Hsu's database structure and functions, Mr. Lipoff testified consistently with his declaration, explaining essentially that it is the user's employee or account number that defines where the fingerprint data is stored:

Q. So the account number indicates where the fingerprint is stored because they are stored in association with each other; is that correct?

...

A. THE WITNESS: Well, I think it's – it's more than that. The structure that the database, as Hsu describes it, I believe -- let me see. I think it's in paragraph 20. Let me see if I can find it. Yeah, so in paragraph 20, column 4, the database is basically a table that associates each user number with a stored fingerprint image or selected attributes.

So what this is telling me is the user number, which you – you said we should call the account number, I believe it's the same thing here, is -- is a database, and so the user number is defining the memory location in which the stored fingerprint image will be stored because the structure of the database is one, as indicated here in column 4, that starts with the user number telling you where to find the memory location that has the stored fingerprint image.

IPR2022-01093
Patent 8,620,039 B2

Ex. 1041, 33:16–34:9. When Patent Owner’s counsel pointed out that Hsu’s paragraph 20 did not pertain specifically to enrollment, Mr. Lipoff explained that the database structure and function in paragraph 20 also applies to the enrollment process shown in Figure 4:

A. Paragraph 20 describes the principle [sic] components of the access control unit, which includes the fingerprint database which is the same fingerprint database that’s in – that’s in – I’m sorry. Same fingerprint database that’s in Figure 4. Figure 4 is the previous paragraph of Hsu we were discussing. Paragraph 26 is the enrollment procedure, but by the time you get to the enrollment procedure, Hsu, earlier in paragraph 20, defined the structure of that same database – database item 44 in Figure 4.

Id. at 34:19–35:9.

Summarizing its position, Patent Owner argues that “Hsu merely discloses that the user’s account number and fingerprint data are stored in association with each other. Hsu offers no other teachings as to how the account number and fingerprint data are stored in the database.” PO Resp. 15XX (citing Ex. 2039 ¶¶ 53–54). Considering our analysis and the evidence discussed above, we disagree. We are persuaded that Hsu does, in fact, explain *how* the account number and fingerprint data are stored in the fingerprint database. Hsu establishes a memory location for storing the fingerprint data in “association” with an employee or account number, and the “association” is contingent on receiving the employee or account number from Hsu’s card or badge during enrollment. *See* Ex 1003, 7:10–12, Fig. 4. (Hsu explaining that “[t]he account number is stored in the database 44 in association with the user’s fingerprint image data.”).

Overall, we are persuaded, based on Petitioner’s arguments and evidence, including the testimony of Mr. Lipoff, that Hsu’s association of a fingerprint with a user’s underlying account or employee number in a

IPR2022-01093
Patent 8,620,039 B2

database record during enrollment discloses limitation 1[C], namely “defining, dependent upon the received card information, a memory location in a local memory external to the card.”

Patent Owner does not present substantive arguments with respect to the remaining limitations 1[P]–[B] and 1[D]–[E] nor with respect to the combination of Hsu and Sanford. Having reviewed the entirety of the record now before us, specifically the disclosures in Hsu and Sanford, we accept Petitioner’s arguments and evidence with respect to the remaining limitations as our own. Pet. 17–40. We also find that Petitioner and Mr. Lipoff have provided articulated reasoning with evidentiary underpinning as to why an ordinarily skilled artisan would have been motivated to combine the teachings of Hsu and Sanford. Pet. 37–40; Ex. 1003 ¶¶ 108–115.

d) Conclusion as to claim 1

Based on the complete record before us and for the reasons expressed above, we are persuaded that Petitioner has shown by a preponderance of evidence that claim 1 would have been obvious over Hsu and Sanford.

4. Dependent claim 2

Claim 2 depends from claim 1 as it recites “storing a biometric signature according to the enrolment method of claim 1.” Ex. 1001, 12:41–42. Claim 2 specifically recites “[a] method of securing a process at a verification station.” *Id.* at 12:39. Thus, different from the enrollment process of claim 1, claim 2 is directed to a verification process that follows the enrollment process.

Patent Owner does not provide separate substantive arguments with respect to claim 2, mainly arguing that claim 2 contains the same method steps, specifically limitation 1[C], of claim 1 and “[a]s the prior art cited by

IPR2022-01093
Patent 8,620,039 B2

[Petitioner] does not teach this limitation, the cited prior art does not render these dependent claims obvious as a result thereof.” PO Resp. 30.

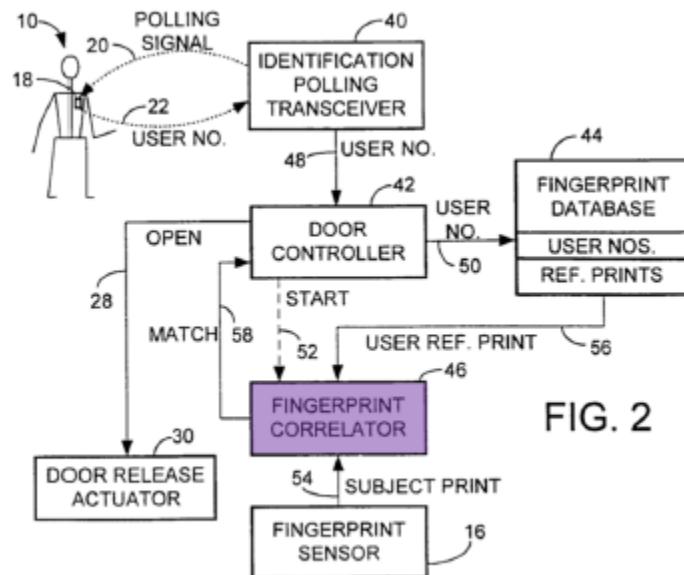
Petitioner argues that Hsu discloses using its system for ATM machines to “conduct banking transactions, such as cash withdrawal or deposit transactions.” Pet. 41 (quoting Ex. 1003 ¶ 24). Petitioner argues specifically, that “[b]ecause a user of Hsu’s system may conduct banking transactions only after her fingerprint is verified, access to the banking transaction process is a verified access.” *Id.*

Claim 2 recites in pertinent part the additional step of:

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

Ex. 1001, 12:45–50.

Petitioner argues that Hsu discloses “fingerprint correlator 46” in Figure 2 as annotated by Petitioner (Pet. 47) and reproduced below.



IPR2022-01093
Patent 8,620,039 B2

Hsu's Figure 2 illustrates diagrammatically the use of fingerprint correlator 46 in conjunction with fingerprint sensor 16 and fingerprint database 44.

Ex. 1003, Fig. 2. Petitioner argues that "fingerprint correlator 46 (purple) 'compares the subject fingerprint from the sensor 16, received over line 54, with the reference fingerprint features received from the database 44 over line 56' to 'determine[] . . . [if] there is a match.'" Pet. 48 (quoting Ex. 1003 ¶¶ 21, 24). Petitioner argues further that because "Hsu's card information (e.g., user number or account number) is used to retrieve the stored biometric signature (e.g., fingerprint) . . . Hsu discloses 'verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the [stored] biometric signature.'" *Id.* at 48–49 (citing Ex. 1006 ¶ 131).

Mr. Lipoff testifies that after enrollment, and because the fingerprint is stored associated with, i.e., "set" or "established" by the employee number or account number in a database record, "Hsu discloses 'verifying the subsequently presented presentation of the card information [e.g., Hsu's account or user number] and the biometric signature [e.g., Hsu's fingerprint] if the subsequently presented biometric signature [e.g., Hsu's fingerprint] matches the biometric signature at the memory location.'" Ex. 1006 ¶ 133.

Petitioner's arguments and Mr. Lipoff's testimony are consistent with Hsu's disclosure. For example, Hsu expressly describes a verification procedure using a stored fingerprint:

The correlator 46 then rapidly compares the subject fingerprint from the sensor 16, received over line 54, with the reference fingerprint features received from the database 44 over line 56. If the correlator 46 determines that there is a match, a match signal is transmitted to the door controller 42 over line 58,

and the controller generates an “open” signal on line 28 to the door release actuator 30.

Ex. 1003, 5:22–29. For dependent claim 2, we have considered and, on the complete record before us, in addition to our analysis above, accept as our own, Petitioner’s arguments and evidence set forth at pages 40–49 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 2 would have been obvious over Hsu and Sanford.

5. Independent claim 13 and dependent claim 14

Independent claim 13 is an apparatus claim reciting “[a] biometric card pointer enrolment system,” and includes similar limitations as independent claim 1. Ex. 1001, 13:67. Different from claim 1, claim 13 also recites “a card device reader,” “a biometric reader,” and for the remaining limitations recites “means for” along with the same functional language as in limitations 1[C]–[E].

Petitioner argues that besides disclosing the biometric pointer system, “Hsu’s biometric card pointer system is also an enrollment system that allows users to be enrolled.” Pet. 49–50 (citing Ex. 1006 ¶¶ 68–74, 136). Petitioner points to Hsu’s “bank card reader 62,” and “fingerprint sensor 16 to account for the recited card and biometric readers in claim 13. *Id.* at 50–51. Considering the “means for” limitations in the remainder of the claim, Petitioner points to the requisite function and structure, for example, for limitation 13[C] Petitioner explains that

[t]he function of this limitation is “defining, dependent upon the received card information, a memory location in a local memory external to the card.”

Id. And for the structure:

Structure corresponding to the claimed means is a computer system with a processor executing an application that uses any segment of card information 605 from a card 601 (1) as a memory reference as shown in Fig. 4 or (2) to determine a group of associated memory references or 3) all equivalents of (1) and (2). Structure is found in '039 Patent, col. 6, line 66 – col. 7, line 23; col. 7, lines 31-35, 39-42, 47-48; col. 8, lines 44-46; col. 11, lines 29-37; col. 12, lines 1-9; Fig. 4.

Id. at 51–52. Petitioner argues that “as explained for Limitation 1[C], Hsu discloses the recited function” which is “defining, dependent upon the received card information, a memory location in a local memory external to the card.” *Id.* at 52. For the structure, Petitioner asserts that “Hsu discloses or renders obvious that fingerprint matching is performed by computer processors executing software/application . . . [f]or example, Hsu discloses using ASIC capable of ‘parallel processing’ for fingerprint verification.” *Id.* at 53 (citing Ex. 1006 ¶23). And, Petitioner argues “Hsu discloses using card information to determine a group of memory references, which are associated because they correspond to the same user.” *Id.* (citing Ex. 1006 ¶ 149).

Apart from its arguments with respect to independent claim 1[C], Patent Owner does not dispute Petitioner’s evidence that Hsu, and Hsu in view of Sanford, disclose and teach the limitations of independent claim 13. *See generally* PO Resp. And, in addition to being persuaded that Hsu discloses the necessary structure and function intimated by “means for,” we find that Hsu renders obvious limitation 13[C] for the same reasons as limitation 1[C]. Based on our review, we find that the complete record fully supports Petitioner’s showing that Hsu and Sanford disclose all the limitations of claim 13. Pet. 49–56.

Dependent claim 14, similar to claim 2, relates to a “verified access system” including “means for verifying (i) a subsequent presentation of card information to the card device reader . . . and (ii) a subsequent presentation of a biometric signature to the biometric reader.” Ex. 1001, 14:10–21. Mr. Lipoff testifies that with respect to “means for verifying,” “Hsu discloses the recited function, for the same reasons I explained for Limitation 2[C].” Ex. 1006 ¶ 174. And for structure, Mr. Lipoff testifies that a person of ordinary skill in the art “would have understood that the verification process in Hsu (*i.e.*, comparing an inputted fingerprint to a stored fingerprint) would or could obviously be accomplished by at least one processor executing an application.” *Id.* ¶ 175.

For dependent claim 14, we have considered and on the complete record before us, accept as our own, Petitioner’s arguments and evidence set forth at pages 57–60 of the Petition. After weighing all relevant factual findings, including the level of ordinary skill in the art, the scope and content of Hsu and Sanford, and any differences between Hsu, Sanford and the claimed invention, we conclude that Petitioner demonstrates by a preponderance of the evidence that claims 13 and 14 of the ’039 patent are unpatentable as obvious over Hsu and Sanford under 35 U.S.C. § 103(a).

6. *Claims 19 and 20*

Independent claim 19 and dependent claim 20 include essentially the same limitations as claims 1 and 2, except, that the preamble to claim 19 recites:

A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

IPR2022-01093
Patent 8,620,039 B2

Ex. 1001, 15:25–16:2. And, for example, the limitation of “receiving card information,” in independent claim 1, is recited in independent claim 19 as “code for receiving card information.”

Petitioner argues that Hsu “discloses various components of its biometric card pointer system (*e.g.*, access control unit) in Figs. 2, 3, and 4, such as a card reader, a fingerprint sensor, a door/access controller, a fingerprint correlator, and a fingerprint database.” Pet. 60. Petitioner argues further that Sanford specifically describes a system that “includes a processor. The processor may be, for example, a computer, workstation, mainframe, pocket PC, personal digital assistant, etc. The processor also preferably includes or is in communication with a verification process 22 and database 24. Verification process 22 may be a software-implemented process that communicates with database 24.” *Id.* at 61 (quoting Ex. 1004 ¶ 18). Based on such disclosures, Mr. Lipoff testifies that a person of ordinary skill in the art “would have understood that the Hsu-Sanford system includes a processor running computer programs stored on a non-transitory computer readable medium.” Ex. 1006 ¶ 179.

Mr. Lipoff’s testimony as to what a person of ordinary skill in the art would understand in regards to the known internals, programming instructions, and memory structure for a biometric card enrollment and verification system is unrebutted on this record.

Petitioner’s arguments and evidence are in all other respects the same as the arguments and evidence presented with respect to claims 1 and 2. We have considered, and on the complete record before us, accept as our own, Petitioner’s arguments and evidence set forth at pages 60–73 of the Petition as to claims 19 and 20. Accordingly, we determine that Petitioner has

IPR2022-01093
Patent 8,620,039 B2

shown by a preponderance of the evidence that claims 19 and 20 would have been obvious over Hsu and Sanford for the same reasons as claims 1 and 2.

E. Ground 2: Claims 1, 2, 13, 14, 19 and 20 in view of Hsu, Sanford, and Tsukamura

Because we determine that claims 1, 2, 13, 14, 19, and 20 would have been obvious over Hsu and Sanford, we need not address these same claims 1, 2, 13, 14, 19, 20 as obvious over Hsu, Sanford, and Tsukamura.

F. Patent Owner's continued 315(b) arguments

In their Response, Patent Owner reiterates their 315(b) argument that we previously addressed in our Institution Decision. PO Resp. 30–47; Inst. Dec. 9–34. Now, Patent Owner argues that in our prior decision we placed too much weight on a lack of control of the proceedings by Apple, and that “[r]ather, a key to the RPI analysis is whether Apple and Petitioners have a structured, preexisting business relationship and whether Apple would receive more than a merely generalized benefit if trial is instituted.” PO Resp. 34 (citing *Applications in Internet Time, LLC v. RPX Corp.*, 897 F.3d 1336, 1351 (Fed. Cir. 2018)).

As an initial matter, we think that Patent Owner's argument mischaracterizes, or at least oversimplifies the holding in *AIT*. In *AIT*, the Federal Circuit admonished the Board for (1), making “certain factual findings that are not supported by substantial evidence,” and (2) “fail[ing] to adhere to the expansive formulation of ‘real party in interest’ that is dictated by the language, structure, purpose, and legislative history of § 315(b).” *AIT*, 897 F.3d at 1351. The Federal Circuit explained in *AIT* that the Board failed to appreciate, among other things, the specific nature of the relationship between RPX and Salesforce, “that RPX, . . . is a for-profit company whose clients pay for its portfolio of ‘patent risk solutions.’” *Id.*

IPR2022-01093
Patent 8,620,039 B2

The Court stated that “the Board did not consider these facts, which, taken together, imply that RPX can and does file IPRs to serve its clients’ financial interests, and that a key reason clients pay RPX is to benefit from this practice in the event they are sued by an NPE.” *Id.* at 1352. As discussed below, we have not overlooked the facts and evidence surrounding the parties’ relationship nor failed to consider the parties’ litigation efforts in the district courts. To the extent Patent Owner has raised valid arguments that may have not been clearly addressed by the Board, we provide the following additional analysis.

With respect to point (1), it is important, factually, that the developer-distributor business relationship between Petitioner and Apple contrasts sharply with the specific intent of the NPE patent portfolio litigation relationship between RPX and Salesforce. As we described in our Institution Decision, Petitioner’s product “Yale Smart Locks”, including “the Yale Assure Lock uses a software application (‘App’) on one’s mobile phone, here on an iPhone sold by Apple, to lock and unlock doors. The App is developed by Petitioner, or one of its business partners, and distributed to iPhone users through the Apple App store.” Inst. Dec. 16. The Developer Agreement (the “Agreement”) between Petitioner and Apple mainly provides “a limited license” to use Apple software “to develop and test” the developer’s software applications for integration on Apple’s iOS platforms. Ex. 2009. Importantly, different from *AIT*, in this case we have before us no facts or evidence showing that the intent, express or otherwise, of the Agreement between Petitioner and Apple is *fundamentally* based on

IPR2022-01093
Patent 8,620,039 B2

protecting one party or the other from patent litigation.⁹ To the extent Patent Owner now argues that we did not appreciate all of its arguments and evidence as to the parties underlying actions in related district court proceedings, we address that matter in due course below. Before doing so, we turn to point (2), and whether, in this case, our Institution Decision appropriately considered the “expansive formulation of ‘real party in interest.’” *AIT*, 897 F.3d at 1351.

In *AIT*, the Federal Circuit explained that the “Board’s determination that Salesforce was not a real party in interest under § 315(b) relied on an impermissibly narrow understanding of the common-law meaning of the term.” *Id.* at 1357. For one thing, the Court pointed out that “an agent with an ownership interest in the subject matter of the suit, or one who is the trustee of an express trust or a party in whose name a contract has been made for the benefit of another, may qualify as a real party in interest.” *Id.* In this proceeding, Patent Owner has failed to point to any persuasive evidence, apart from software compatibility with Apple’s iOS platforms as discussed in the Agreement, that Apple has any overt interest, influence, development or design influence over Petitioner’s “Yale Smart Locks” products or App. In addition, Patent Owner has produced no evidence that Apple holds any ownership interest, assets, or expressly administers any property rights as a trustee or agent for the benefit of Petitioner indicative of real party in interest relationships under common law.

⁹ We acknowledge that the Agreement contains representations and warranties of noninfringement, as well as indemnification clauses. Ex. 2009, 16, 41–43. We consider that these clauses are perhaps best understood, at least from Apple’s perspective as a distributor, as mechanisms to avoid liability should the need arise, rather than tools exerting control or perpetuating an agency relationship with Petitioner.

IPR2022-01093
Patent 8,620,039 B2

Essentially the entirety of the evidence of the business relationship in this proceeding is contained within the Agreement which we already discussed in detail in our Institution Decision. Inst. Dec, 9–34. For example, there is an indemnification clause that requires Petitioner to

[u]pon Apple’s request, defend, Apple, its directors, officers, employees, independent contractors and agents (each an “Apple Indemnified Party”) from any and all claims, losses, liabilities, damages, taxes, expenses and costs, including without limitation, attorneys’ fees and court costs (collectively, “Losses”), incurred by an Apple Indemnified Party and arising from or related to . . . any claims that Your Covered Product or the distribution, sale, offer for sale, use or importation of Your Covered Product (whether alone or as an essential part of a combination), Licensed Application Information, metadata, or Pass Information violate or infringe any third party intellectual property or proprietary rights;

Id. at 43. There is no evidence in this case that Apple has invoked their rights under this clause, nor has Patent Owner argued or explained how this clause or the parties’ actions before the Board and in the underlying district court litigation implicate a common law agency relationship between the parties. An agency relationship could potentially occur if Apple were to request Petitioner to step in and defend it. Yet Patent Owner has provided no argument or persuasive evidence that such is the case here. Apple has, in fact, committed to its own defense by filing its own IPR, e.g., IPR2022-00600, against Patent Owner. Moreover, compelling evidence provided by Petitioner in this case is exactly the opposite, and avers under penalty of perjury that “[t]here have been no communications between Petitioners and Apple, directly or through counsel, relating to indemnification or obligation to indemnify based on assertion of . . . U.S. Patent No. 8,620,039) (*id.* at 11–12).” Ex. 1023, 8–9, 14.

IPR2022-01093
Patent 8,620,039 B2

We recognize that Apple may derive some benefit if additional claims of the '039 patent are determined to be unpatentable in this proceeding. This derived benefit does not, however, make Apple an RPI to this proceeding.

See WesternGeco LLC v. ION Geophysical Corp., 889 F.3d 1308, 1321 (Fed. Cir. 2018) (stating in the context of the broader concept of privity that “[a]s a general proposition, we agree with the Board that a common desire among multiple parties to see a patent invalidated, without more, does not establish privity”).

On the facts and evidence before us in this proceeding it is the Agreement, analyzed here and in our Institution Decision, that best explains the business relationship between the parties. The Agreement sets forth with reasonable clarity the specific expectations of the parties, mainly that (a) Petitioner is allowed “a limited license to use the Apple Software and Services provided to You under this Program to develop and test Your Applications on the terms and conditions set forth in this Agreement;” and (b) “Applications that meet Apple’s Documentation and Program Requirements may be submitted for consideration by Apple for distribution via the App Store, Custom App Distribution, or for beta testing through TestFlight.” Ex. 2009, 1. Accordingly, the evidence leads us to conclude that Apple is a distributor of Petitioner’s App for use with Petitioner’s “Yale Smart Lock” products, and without more, that is about all that can be said about the relationship.

We turn, below, to particular facts in this case that Patent Owner argues the Board overlooked in our Institution Decision.

During oral argument Patent Owner’s counsel raised an issue concerning our earlier conclusion in our Institution Decision that Apple is *not* a real party in interest to this proceeding or a privy with Petitioner. Inst.

IPR2022-01093
Patent 8,620,039 B2

Dec. 28; Tr. 45–46. Counsel contends “there is an inconsistency between [Petitioner’s], you know, assertions regarding Apple in the [Declaratory Judgment] complaint. And then in defending the RPI position.” Tr. 45:20–23. Specifically, counsel explained that they “didn’t see that the Board specifically considered our argument that it’s relevant that ASSA ABLOY filed the DJ complaint with respect to the ’039 patent, even though the ’039 patent had never been raised by Patent Owner to ASSA ABLOY.” *Id.* at 46:3–6. Counsel further argued that the present “situation mirror[s] the situation in the *Worlds v. Bungie* case, where a very similar fact pattern was considered relevant by the [F]ederal [C]ircuit.” *Id.* at 46:7–9; *see also* *Worlds Inc. v. Bungie, Inc.*, 903 F.3d 1237, 1239 (Fed. Cir. 2018) (“*Bungie*”) (determining that because “the Board erred in its real-party-in-interest analysis, we vacate its decisions and remand for proceedings consistent with this opinion”).

As an initial matter, our analysis of Petitioner’s section 315(b) time-bar arguments in our Institution Decision covers 20 pages and considers in detail evidence submitted by both parties regarding business relationships and the Apple Developer License Agreement, i.e., the “Agreement,” (Ex. 2009) including warranties, indemnification, product inspection and insurance, between Petitioner and Apple. Inst. Dec. 9–29. For example, as it relates to Patent Owner’s issue raised here, we noted that “[i]n the Declaratory Judgment complaint, Petitioner states, ‘[CPC] is also engaged in an aggressive litigation campaign that includes Apple Inc. (‘Apple’), a business partner of [Petitioner].’” *Id.* at 14. We explained that

[t]he business relationship between Apple and Petitioner is that Petitioner, or one of the named entities collectively referred to as Petitioner, makes products that interface with Apple products and may be sold on Apple’s website. For example, ASSA

ABLOY Residential Group, Inc., a named entity included as a Petitioner in this proceeding, makes and sells security locks under the brand name “Yale” . . . the Yale Assure Lock uses a software application (“App”) on one’s mobile phone, here on an iPhone sold by Apple, to lock and unlock doors. The App is developed by Petitioner, or one of its business partners, and distributed to iPhone users through the Apple App store.

Id. at 14–15. Thus, in our Institution Decision, we did consider the fact that Petitioner, in its Declaratory Judgment Complaint, admitted to being a business partner with Apple. We also considered the fact that as part of the business relationship Petitioner entered into the Agreement. *Id.* at 18. We considered critical clauses in the Agreement such as the representations and warranties clause explaining that “[w]e do *not* consider Section 3.2(d) to be a ‘warranty.’ It is not a guarantee that products will not infringe. It is a representation of the developer’s current ‘knowledge and belief.’ It is far different from the obligations created by the App developer’s agreement in *Bungie*.¹” *Id.* at 19.

With respect to indemnification, we determined that the Agreement did in fact contain an indemnification clause, which *could* be implemented “upon Apple’s request.” *Id.* at 22. However, also different from the facts in *Bungie*, in this case we have sworn interrogatories provided by Petitioner presenting strong evidence that “[t]here have been no communications between Petitioners and Apple, directly or through counsel, relating to indemnification or obligation to indemnify based on assertion of . . . U.S. Patent No. 8,620,039.” *Id.* at 23 (quoting Ex. 1023, 11–12).

Patent Owner now urges us to also consider the fact that its cease-and-desist letters to Petitioner, i.e., the “Yale Letters” (Exs. 2005, 2006), never threatened Petitioner with infringement of the ’039 patent, only U.S. Patent Nos. 9,665,705 and 9,269,208. *See* Prelim. Resp. 7 (Patent Owner arguing

IPR2022-01093
Patent 8,620,039 B2

that it “never raised or otherwise mentioned the ’039 Patent to Yale or any of the Petitioners at any time” (citing Ex. 2008). This is a concern, Patent Owner contends, because Petitioner filed its Declaratory Judgment Complaint admitting to a business relationship with Apple as well as this IPR, and both proceedings challenge the ’039 patent. *See* Ex. 2007 ¶ 2 (Petitioner stating in its Declaratory Judgment Complaint that “[t]he ASSA ABLOY Entities seek a declaration of non-infringement of U.S. Patent Nos. 9,269,208 (“the ’208 Patent”), 9,665,705 (“the ’705 Patent”), and 8,620,039 (“the ’039 Patent”) (collectively, the “Patents-in-Suit”)).

This argument is frankly somewhat undeveloped in Patent Owner’s explanations of the facts and background in its Preliminary Response. Prelim. Resp. 5–10. We acknowledge that Petitioner was apparently never overtly threatened with infringement of the ’039 patent. Ex 2005; Ex. 2006. Yet Patent Owner fails to persuasively explain *why* Petitioner’s challenges to the ’039 patent in the Declaratory Judgment Complaint weigh in favor of finding a privy or a real party-in-interest relationship between Petitioner and Apple. *See* Prelim. Resp. 7 (Patent Owner arguing largely that “Patent Owner never raised or otherwise mentioned the ’039 Patent to Yale or any of the Petitioners at any time”). As we understand the argument, Patent Owner alleges that because it never threatened Petitioner with the ’039 patent, Petitioner is now, without provocation, doing Apple’s bidding and working at Apple’s behest by challenging the ’039 patent in the Declaratory Judgment Complaint and in these *inter partes* review proceedings. It is also not clearly explained why the inclusion of Petitioner’s related entities of ASSA ABLOY Global Solutions, Inc. (‘Hospitality’), and HID Global Corporation, in these IPR proceedings as real parties-in-interest and also in the Declaratory Judgment Complaint, matters as to the relationship between

IPR2022-01093
Patent 8,620,039 B2

Petitioner and Apple. *See* Prelim. Resp. 8 (Patent Owner's arguing that "Petitioners also filed the Declaratory Judgment Complaint as to HID and Hospitality, whom Patent Owner had never contacted regarding the patents or technology at issue") (citing Ex. 2005; Ex. 2006; Ex. 2008).

Two things can be true. Petitioner can have a business relationship with Apple and both parties can have a legitimate interest in defending themselves separately in litigation. We do not find anything in Petitioner's Declaratory Judgment Complaint that alters our prior decision in this regard. The fact that Petitioner and each of its entities were not explicitly threatened with infringement allegations in the Yale Letters as to the '039 patent does not mean that Patent Owner would never assert infringement against Petitioner based on the '039 patent claims. Ex. 2005; Ex. 2006. This is especially true in light of the fact that Patent Owner asserted the '039 patent against Apple in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, No. 3:22-cv-02553, apparently due to or resulting from the products that Petitioner makes, uses, and sells through Apple's electronic device platforms. Ex. 2007 ¶ 44 ("On February 23, 2021, [Patent Owner] asserted all three of the Patents-in-Suit against Apple.").

On the facts here, we conclude that filing a declaratory judgment action or an *inter partes* review to challenge the claims of a patent, i.e., the '039 patent, that was asserted against a third party, but based on Petitioner's product, is a reasonable litigation strategy for Petitioner independently. The declaratory judgment action filing itself does not demonstrate some sort of heightened collusion even where a benefit inures to a party with whom Petitioner has a business relationship. Patent Owner has not explained, for instance, that, but for Apple's technology or actions, Petitioner has no actionable reason to challenge the patentability of the '039 patent claims.

IPR2022-01093
Patent 8,620,039 B2

See, generally, Prelim. Resp. Also, by way of example, Patent Owner argues in its Preliminary Response that in the Declaratory Judgment Complaint, “Petitioners further asserted that ‘it is highly likely that Charter Pacific will sue the Assa Abloy Entities *on the same patents that have been asserted against Apple.*’” Prelim. Resp. 22 (quoting Ex. 2007 ¶30). In our view, this assertion is primarily offered in the Complaint to show Petitioner’s apprehension of litigation because it admittedly makes, uses, and sells products potentially covered by the claims in the same three patents through Apple’s platforms. Patent Owner does not explain persuasively why Petitioner would not have been concerned about infringing the ’039 patent, nor why such apprehension shows any more intimate relationship than we considered in our Institution Decision. The mere fact that an accused infringer, in this case Petitioner, files a declaratory judgment action explaining its business relationship with Apple and offering reasons supporting the declaratory judgment action with respect to the same three patents that Apple is accused of infringing, does not, without more, establish persuasive additional information or substantive facts that we failed to consider in our original analysis.

Overall, and on the complete record before us we do not find that any of Petitioner’s assertions in its Declaratory Judgment Complaint change our underlying conclusion that Petitioner and Apple are not in privy or real parties in interest. *See* Inst. Dec. 34 (determining that “[t]he totality of the evidence before us does not establish anything other than a traditional business relationship between Apple and Petitioner”).

III. CONCLUSION¹⁰

For the reasons discussed above, we determine Petitioner meets its burden of establishing, by a preponderance of the evidence, that the challenged claims are unpatentable, as summarized in the following table:

Claims	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1, 2, 13, 14, 19, 20	103(a)	Hsu, Sanford	1, 2, 13, 14, 19, 20	
1, 2, 13, 14, 19, 20	103(a)	Hsu, Sanford, Tsukamura ¹¹		

III. ORDER

For the reasons given, it is

ORDERED that, based on a preponderance of the evidence, claims 1, 2, 13, 14, 19, and 20 of the '039 patent have been shown to be unpatentable; and

¹⁰ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. §§ 42.8(a)(3), (b)(2).

¹¹ Because Petitioner's contentions regarding the obviousness of claims 1, 2, 13, 14, 19, and 20 in view of Hsu and Tsukamura are dispositive of these challenged claims, we do not reach asserted ground 2. *See In re Gleave*, 560 F.3d. at 1338.

IPR2022-01093
Patent 8,620,039 B2

FURTHER ORDERED that, because this is a Final Written Decision, any party to the proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2022-01093
Patent 8,620,039 B2

For PETITIONER:

Dion Bregman
Andrew Devkar
James Kritsas
MORGAN, LEWIS & BOCKIUS LLP
dion.bregman@morganlewis.com
andrew.devkar@morganlewis.com
james.kritsas@morganlewis.com

PATENT OWNER:

Andrew Ryan
CANTOR COLBURN LLP
aryan@cantorcolburn.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASSA ABLOY AB, ASSA ABLOY INC.,
ASSA ABLOY RESIDENTIAL GROUP, INC., AUGUST HOME, INC.,
HID GLOBAL CORPORATION, and
ASSA ABLOY GLOBAL SOLUTIONS, INC.,
Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY, LTD,
Patent Owner.

IPR2022-01094
Patent No. 8,620,039 B2

Before SCOTT A. DANIELS, AMBER L. HAGY and
FREDERICK C. LANEY, *Administrative Patent Judges*.

DANIELS, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global Corporation, and ASSA ABLOY Global Solutions, Inc., (“ASSA” or “Petitioner”) filed a Petition requesting *inter partes* review (“IPR”) of claims 3–12 and 15–18 of U.S. Patent No. 8,620,039 B2 (Ex. 1001, “the ’039 patent”). Paper 2 (“Pet”). CPC Patent Technologies PTY, Ltd., (“CPC” or “Patent Owner”) filed a Preliminary Response to the Petition. Paper 11 (“Prelim. Resp.”). Petitioner filed a Reply to Patent Owner’s Preliminary Response. Paper 15 (“Prelim. Reply”). Patent Owner filed a Sur-Reply to Petitioner’s Reply. Paper 18 (“Prelim. Sur-Reply”).

Following our Institution Decision (Paper 20, “Inst. Dec.”), in which we determined that Petitioner was *not* time-barred from filing its Petition, Patent Owner filed a Response. Paper 23 (“PO Resp.”). *See* Inst. Dec. 9–34. Petitioner filed a Reply. Paper 25 (“Pet. Reply”). Patent Owner filed a Sur-Reply. Paper 29 (“PO Sur-Reply”). An oral hearing was held on November 9, 2023. A transcript of the hearing has been entered as Paper 35. (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a). For the reasons explained below, we determine that Petitioner has met its burden of showing by a preponderance of the evidence that claims 3–12 and 15–18 are unpatentable.

A. *Real Parties in Interest*

Petitioner states that ASSA ABLOY AB, ASSA ABLOY Inc., ASSA ABLOY Residential Group, Inc., August Home, Inc., HID Global Corporation, and ASSA ABLOY Global Solutions, Inc., are the real parties

IPR2022-01094
Patent 8,620,039 B2

in interest.¹ Pet. 1. Patent Owner states that CPC Patent Technologies PTY, Ltd., is the real party in interest. Paper 4, 2.

B. Related Matters

Petitioner indicates that it filed a declaratory judgment against Patent Owner with respect to the '039 patent in *ASSA ABLOY AB, et al. v. CPC Patent Technologies Pty Ltd., et al.*, No. 3-22-cv-00694, in the United States District Court for the District of Connecticut. Pet. 1–2. And Petitioner points out that the '039 Patent is asserted against Apple, Inc., in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, No. 3:22-cv-02553, in the United States District Court for the Northern District of California, San Jose Division. *Id.* Petitioner points out that Apple challenged the '039 patent in IPR2022-00600. *Id.* at 2. On October 13, 2023, we entered a Final Written Decision (Paper 22) in IPR2022-00600 finding claims 1, 2, 19, and 20 of the '039 patent invalid for obviousness. Concurrently with this Decision, in IPR2022-01093, we determine that claims 1, 2, 13, 14, 19, and 20 of the '039 patent are invalid for obviousness.

In addition to the proceedings noted by Petitioner, Patent Owner indicates that “the following judicial and/or administrative matters [] may affect, or be affected by, a decision in this proceeding.” *CPC Patent Technologies PTY Ltd. v. HMD Global Oy*, Case No. 6:21-cv-00166 in the United States District Court for the Western District of Texas; IPR2022-00600; IPR2022-00601; IPR2022-00602; IPR2022-01006; IPR2022-01045; IPR2022-01089; and IPR2022-01093. Paper 4, 2–3.

¹ In its Declaratory Judgment Complaint against Patent Owner, Petitioner also refers to ASSA ABLOY Global Solutions, Inc., as “ASSA ABLOY Global Solutions, Inc. (‘Hospitality’).” Ex. 2007, 2.

C. *The '039 Patent (Ex. 1001)*

The '039 patent, titled “Card Device Security Using Biometrics,” relates to a biometric card pointer (BCP) system intended to more efficiently and securely permit a user to store biometric information during a user enrollment phase, and in future verification processes permits the user access their account using an identification (ID) card and biometric information such as a fingerprint. Ex. 1001, code (54), 2:51–3:11.

The '039 patent explains that in the enrollment phase “[t]he card user’s biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase).” *Id.* at 2:62–64. The '039 patent explains further that “[t]he biometric signature is stored at a memory address defined by the (‘unique’) card information on the user’s card as read by the card reader of the verification station.” *Id.* at 2:64–67. Following the enrollment phase, the '039 patent describes that

[a]ll future uses (referred to as uses in the verification phase) of the particular verification station by someone submitting the aforementioned card requires the card user to submit both the card to the card reader and a biometric signature to the biometric reader, which is verified against the signature stored at the memory address defined by the card information thereby determining if the person submitting the card is authorised to do so.

Id. at 3:4–11.² For both enrollment and future uses, the use of the ID card at a verification station “is identical from the card user’s perspective, requiring

² The words “enrolment,” “authorise,” and “authorisation” are the British spellings of “enrollment,” “authorize,” and “authorization.” *See, e.g.*, <https://www.merriam-webster.com/dictionary/authorisation>, last visited Jan.

IPR2022-01094
Patent 8,620,039 B2

merely input of the card to the card reader, and provision of the biometric signature ([e.g.] thumb print or retinal scan etc.) to the biometric reader.” *Id.* at 3:12–15.

Figure 4 of the '039 patent is reproduced below.

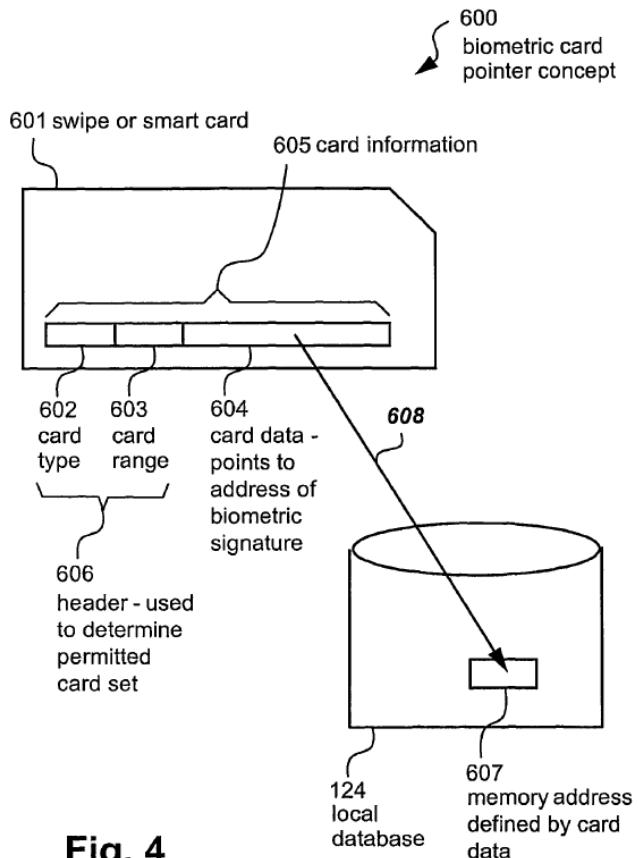


Fig. 4

Figure 4, of the '039 patent, above, illustrates swipe or smart card 601 including card information 605 encompassing fields for card type 602, card range 603, and card data 604. The '039 patent describes that “the card data 604 acts as the memory reference which points, as depicted by an arrow 608,

5, 2023. We will use the American English spelling of these words except where quoted from the '039 patent.

IPR2022-01094
Patent 8,620,039 B2

to a particular memory location at an address 607 in the local database 124.” *Id.* at 7:31–35. Information 605 can be encoded on a magnetic strip on the card, for example. *Id.* at 7:28–29. The ’039 patent explains that for a specific user “[i]n an initial enrolment phase, . . . [t]he card data 604 defines the location 607 in the memory 124 where their unique biometric signature is stored.” *Id.* at 7:43–49. And, the ’039 patent explains further that “in later verification phases, . . . [t]his signature is compared to the signature stored at the memory location 607 in the memory 124, the memory location 607 being defined by the card data 604 read from their card 601 by the card reader 112.” *Id.* at 7:50–56.

Figures 6 and 7, reproduced below, depict the differences between verification process 205 shown in Figure 6, and enrollment process 207 shown in Figure 7.

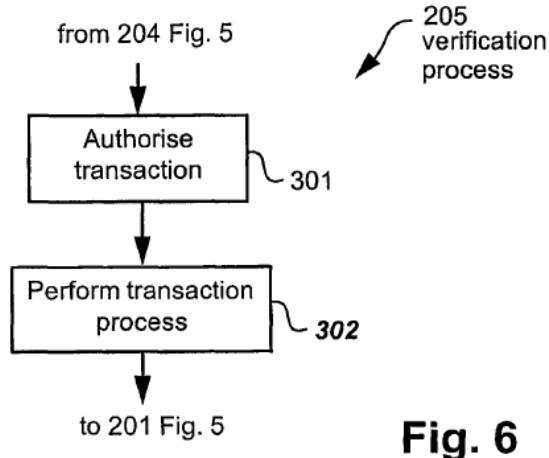


Figure 6 illustrates verification process 205, which occurs after the enrollment process, illustrated below in Figure 7.

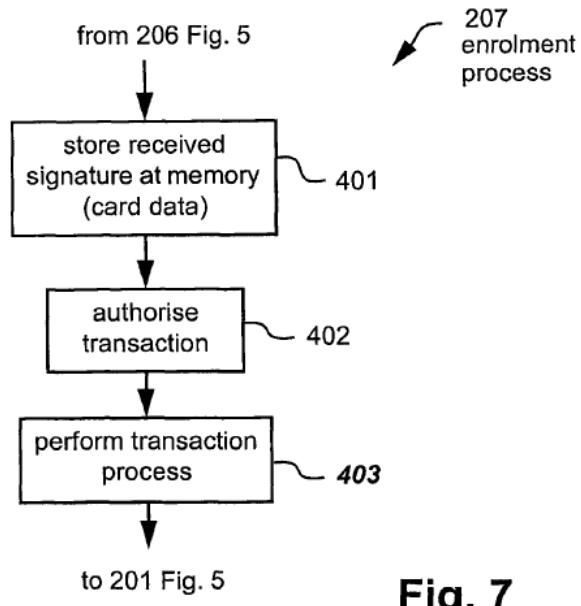
**Fig. 7**

Figure 7 of the '039 patent illustrates enrollment process 207 where the system at “step 401 stores the biometric signature received by the step 203 in the memory 124 at a memory address defined by the card data 604.” *Id.* at 9:64–66 (referring to elements 203 and 124 described in Figure 5). Figure 6 illustrates that verification process 205

is entered from the step 204 in FIG. 5, after which a step 301 authorises the transaction. This authorisation step 301 indicates that the biometric signal received by the biometric reader 102 in the step 203 matches the biometric signature previously stored in the local database 124 by a previous enrolment process 207.

Id. at 9:43–48. Then, “step 204 reads the contents stored at a single memory address defined by the card data 604 and checks these contents against the biometric signature received in the step 203.” *Id.* at 8:34–37.

A difference between verification process 205 and enrollment process 207 is that the enrollment process includes step 401, which *stores* the biometric signature “at a memory address defined by the card data 604,” whereas in verification process 205 “step 204 *reads* the contents stored at a

IPR2022-01094
Patent 8,620,039 B2

single memory address defined by the card data 604” and compares the stored biometric signature with the input biometric signature. *Id.* at 9:65–66, 8:24–26 (emphasis added).

D. Illustrative Claim

Claims 3, 15, and 18 are independent. Each of claims 4–12 and 16–17 depends, respectively, from independent claims 3 and 15. Claim 3, a method claim, illustrates the claimed subject matter and is reproduced below with certain limitations of interest in italics:³

3. 3[P] A method of securing a process at a verification station, the method comprising the steps of:

3[A] (a) providing card information from a card device to a card reader in the verification station;

3[B] (b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

3[C] (c) determining if the provided card information has been previously provided to the verification station;

3[D(P)] (d) *if the provided card information has not been previously provided to the verification station;*

3[D(1)] (da) *storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and*

3[D(2)] (db) performing the process dependent upon the received card information;

3[E(P)] (e) if the provided card information has been previously provided to the verification station;

3[E(1)] (ea) comparing the inputted biometric signature to the biometric signature stored in the memory at

³ We adopt and have applied Petitioner’s alphanumeric designations for the elements of the challenged claims. *See, e.g.*, Pet. 12–36.

IPR2022-01094
Patent 8,620,039 B2

the memory location defined by the provided card information;

3[E(2)] (eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

3[E(3)] (ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

Ex. 1001, 11:67–14:21. The limitations 3[A]–3[E(3)] are similarly recited in independent claim 15 as an apparatus claim for “[a] verification station for securing a process,” and also in independent claim 18 in the context of “[a] non-transitory computer readable medium.” *Id.* at 14:23–46, 14:64–15:24.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–12 and 15–18 would have been unpatentable based on the following grounds:

Ground	Claim(s) Challenged	35 U.S.C. § ⁴	Reference(s)/Basis
1	3, 4, 6–11, 15, 16, 18	103(a)	Sanford, ⁵ Hsu, ⁶
2	3, 4, 6–11, 15, 16, 18	103(a)	Sanford, Hsu, Tsukamura ⁷
3	5	103(a)	Sanford, Hsu, Leu ⁸

⁴ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 296–07(2011), took effect on September 16, 2011. The changes to 35 U.S.C. §§ 102 and 103 in the AIA do not apply to any patent application filed before March 16, 2013. Because the application for the patent at issue in this proceeding has an effective filing date before March 16, 2013, we refer to the pre-AIA version of the statute.

⁵ Ex. 1004, PCT Appl’n No. PCT/US03/07238 (pub. Sept. 18, 2003).

⁶ Ex. 1003, European Patent Appl’n No. EP 0924655 A2 (pub. June 23, 1999).

⁷ Ex. 1005, US Patent No. 6,963,660 B1 (Nov. 8, 2005).

⁸ Ex. 1008, European Patent Appl’n No. EP O 881 608 A1 (pub. Dec. 2, 1986)

Ground	Claim(s) Challenged	35 U.S.C. § ⁴	Reference(s)/Basis
4	5	103(a)	Sanford, Hsu, Leu, Tsukamura
5	12	103(a)	Sanford, Hsu, Houvener ⁹
6	12	103(a)	Sanford, Hsu, Tsukamura, Houvener
7	17	103(a)	Sanford, Hsu, McCalley ¹⁰
8	17	103(a)	Sanford, Hsu, Tsukamura, McCalley

Petitioner relies on the testimony of Stuart Lipoff. Ex 1006 ¶¶ 1–459. Patent Owner presents the testimony of Samuel Russ, Ph.D. Ex. 2039 ¶¶ 1–72.

II. ANALYSIS

A. Legal Standards

A patent claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. 35 U.S.C. § 103; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). “[W]hen a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result.” *KSR*, 550 U.S. at 416 (citing *United States v. Adams*, 383 U.S. 39, 50–51 (1966)). The question of obviousness is resolved based on underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the

⁹ Ex. 1010, US Patent No. 5,790,674 (Aug. 4, 1998).

¹⁰ Ex. 1011, US Patent No. 5,956,415 (Sep. 21, 1999).

IPR2022-01094
Patent 8,620,039 B2

prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Factors pertinent to a determination of the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology, and (6) educational level of workers active in the field. *Env't'l. Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381–82 (Fed. Cir. 1983)). Not all such factors may be present in every case, and one or more of these or other actors may predominate in a particular case. *Id.* Moreover, these factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. Ltd, Inc. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007).

In determining a level of ordinary skill, we also may look to the prior art, which may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Additionally, the Supreme Court informs us that “[a] person of ordinary skill is also a person of ordinary creativity, not an automaton.” *KSR*, 550 U.S. at 421.

Petitioner proposes that a person of ordinary skill in the art at the time of the '039 patent “would have had at least an undergraduate degree in electrical engineering, or equivalent education, and at least two years of work experience in the field of security and access-control.” Pet. 8 (citing Ex. 1006 ¶ 26).

IPR2022-01094
Patent 8,620,039 B2

Patent Owner offers the level of ordinary skill we adopted in IPR2022-00600, which is that a person of ordinary skill in the art at the time of the '039 Patent

would have had at least a bachelor's degree in computer engineering, computer science, electrical engineering, or a related field, with at least one year of experience in the field of human-machine interfaces and device access security. Additional education or experience might substitute for the above requirements.

PO Resp. 6–7; *see also* IPR2022-00600, Paper 22 at 12 (PTAB October 13, 2023) (Final Written Decision).

In this proceeding, Patent Owner's and Petitioner's levels of ordinary skill in the art, in particular education, are not substantively different. Petitioner's proposal requires at least two years of experience in the field of security and access control, compared to one year as proposed by Patent Owner. We maintain our determination of the level of ordinary skill in the art from IPR2022-00600, including at least one year of experience as Patent Owner urges. On this record, Patent Owner's proposed level of ordinary skill in the art is consistent with our review and understanding of the technology and descriptions in the '039 patent and the asserted prior art references. *See Okajima*, 261 F.3d at 1355. Indeed, the difference between one and two years of experience in the field is fairly minimal considering that neither party asserts that it is necessary to have a significant amount of experience, e.g., 5–10 years in the field. For consistency, we rely on the same level of ordinary skill in the art that we determined in IPR2022-00600.

C. *Claim Construction*

We interpret a claim “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C.

IPR2022-01094
Patent 8,620,039 B2

282(b).” 37 C.F.R. § 42.100(b) (2020). Under this standard, we construe the claim “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.* Furthermore, we expressly construe the claims only to the extent necessary to determine whether to institute *inter partes* review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

1. “*if the provided card information has not been previously provided to the verification station . . . storing the imputed biometric signature*”

Patent Owner argues that the independent claims challenged here, for example limitations 3[D](P)+[D](1)], are specifically directed to an enrollment process, although the word “enrolling” or “enrollment,” is not recited expressly in the claims. PO Resp. 7 (citing Ex. 2039 ¶ 39). Patent Owner argues that a person of ordinary skill in the art “would understand this to be an enrollment process because the user’s card information has not previously been entered into the system and the user’s biometric data has not previously been stored in the system’s memory. *Id.*

Petitioner does not address whether the claims encompass an enrollment process. *See, generally*, Pet.

Because at least Hsu, Sanford, and Tsukamura each discloses an enrollment process, in this case we need not explicitly determine whether the language from which Patent Owner argues infers “enrollment” in claim 3 is limiting. We can agree that from reading the ’039 patent in context there is

a difference between verification process 205 and enrollment process 207.

As we explained in our Institution Decision

the enrollment process includes step 401, which *stores* the biometric signature “at a memory address defined by the card data 604,” whereas in verification process 205 “step 204 *reads* the contents stored at a single memory address defined by the card data 604” and compares the stored biometric signature with the input biometric signature.

Inst. Dec. 7 (citing Ex. 1001, 9:65–66, 8:24–26). The language of the independent claims and the requirement that where the card information has *not* been previously provided, “storing the inputted biometric signature,” tracks with the specification description of an enrollment phase.

See Ex. 1001, 9:63–65 (“The [enrollment] process 207 is entered from the step 206 in FIG. 5, after which a step 401 stores the biometric signature received by the step 203 in the memory 124.”). Therefore, for purposes of this Decision, we will consider the limitations of claims 3, 15, and 18 to include, at least in part, an enrollment process. However, because the terms “enrolling” or “enrollment” do not create any particular dispute between the parties that we need to resolve, we need not determine whether they are, in fact limitations.

2. *“a memory location defined by the provided card information”*

Claim limitation 3[D](1) recites the step of “storing the inputted biometric signature in a memory *at a memory location defined by the provided card information.*” Ex. 1001, 12:61–63 (emphasis added). Patent Owner argues that “the proper construction of [this] claim term is: ‘the system sets or establishes a memory location in a memory, said location being contingent upon or determined by the provided card information.’”

PO Resp. 8. Patent Owner also argues that a person of ordinary skill in the

IPR2022-01094
Patent 8,620,039 B2

art “would interpret the word ‘defined,’ especially in the context of enrollment, to mean ‘setting’ or ‘establishing.’” *Id.*

Petitioner proposes alternative constructions. Petitioner first proposes that “defining” means that “a memory location is somehow determined from (or is dependent on) the card information.” Pet. 9. Petitioner alternatively proposes that “defining” means “a memory location is specified by the card information itself.” *Id.* Petitioner contends that the second construction is most consistent with the specification of the ’039 patent specification. *Id.* According to Petitioner, and considering that the ’039 describes “a biometric card pointer system,” a person of ordinary skill in the art “would have understood that the user’s card information itself specifies the physical memory address (such as by acting as a pointer) for the user’s biometric signature.” *Id.* at 11 (citing Ex. 1006 ¶ 47).

Consistent with our prior decision in IPR2022-00600 and our concurrent decision in IPR2022-01093, we determine also in this proceeding that Patent Owner’s construction is sufficiently accurate.¹¹ *See Apple, Inc. v. CPC Patent Technologies, Ltd.*, IPR2022-00600, Paper 22, 29–39 (Final Written Decision); *see also NTP Inc., v. Research in Motion, Ltd.*, 418 F.3d 1282, 1293 (Fed. Cir. 2005) (noting that, when construing claims in patents that derive from the same parent application and share common terms, “we

¹¹ Different from independent claim 1 addressed in IPR2022-01093 and IPR2022-00600, independent claim 3, and specifically limitation 3[D(1)], does not recite “defining, *dependent upon* the received card information,” but “defined by the provided card information.” *Compare* Ex. 1001, 12:33, *with id.* at 12:63–64. Limitation 3[E(2)] does additionally recite “performing the process *dependent upon* the received card information.” For purposes of claim construction, we do not find the claim language as to these limitations between claims 1 and 3 to be substantively different in scope or meaning nor does either party argue that they are.

IPR2022-01094
Patent 8,620,039 B2

must interpret the claims consistently across all asserted patents”). In our Final Written Decision in IPR2033-00600, we explained that

[c]onsidering the abstract and the specification of the ’039 patent, what “defining, dependent upon . . .” means as a whole, in the context of claim 1 and “a method of enrolling,” is that during an *enrollment* process, the claimed “biometric signature,” e.g., a fingerprint, is not yet stored in the memory and no memory location or address has been “set” or “established” for the fingerprint. When the fingerprint, and then the card, is provided to the system during enrollment, the card information provides data that establishes *where*, e.g., at what memory location or address, the system will *store* the fingerprint data.¹²

IPR2022-00600, Paper 22, 30. We also explained that “[i]mportantly . . . we do not understand that ‘defining . . . a memory location,’ or Patent Owner’s alternative wording, ‘establishing’ or ‘setting,’ means ‘[*creating*] . . . a memory location in a local memory.’” *Id.* at 32. We explained further that “[w]hile we might agree that ‘the memory location cannot [already be defined],’ . . . we do not agree that it ‘cannot already exist.’” *Id.* at 33. During the oral hearing in this proceeding, Patent Owner’s counsel argued that “Patent Owner in this case has not argued that defining means creating.” Tr. 31:3–4. Patent Owner’s counsel argued further, “[a]ll we’re saying that Claim 1 requires is that when a user swipes their card, that is the information that is on the card, not -- in that moment in time, not something else in the

¹² We use the terms “memory location” and “memory address” interchangeably because, in terms of computer memory, an “address” is well-understood as “[a] number specifying a location in memory where data is stored.” MICROSOFT COMPUTER DICTIONARY, 5th Ed. (2002) Microsoft Press.

IPR2022-01094
Patent 8,620,039 B2

system, but the information on the card that directs the system where to store that particular user’s fingerprint or other biometric data.”¹³ *Id.* at 31:7–11.

Considering Patent Owner’s arguments and asserted claim construction with respect to the phrase “memory location defined by the provided card information” and limitation 3[D](1) as a whole, we maintain the claim construction given in IPR2022-00600 for the reasons provided here and in the Final Written Decision in that proceeding. IPR2022-00600, Paper 22, 29–36.

We understand that, during an enrollment process, the claimed “biometric signature,” e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been “defined,” as in “set” or “established,” in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint are received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data. The memory location or address where the fingerprint data is stored is, therefore, “contingent” on the card information, as Patent Owner’s construction requires.

3. *Other claim terms agreed upon and construed by the District Court*

Petitioner indicates that the following terms have been previously agreed to between Apple and Patent Owner:

“*dependent upon*” – Plain and ordinary meaning, defined as “contingent on or determined by”

¹³ We understand in the context of this proceeding that Patent Owner’s counsel’s argument would apply to independent claims 3, 15, and 18 as well as claim 1.

“*biometric signature*” – Plain and ordinary meaning. Pet. 12 (citing Ex. 1013, 2). Patent Owner does not specifically address these terms in its Patent Owner Response.

Considering these constructions and that our analysis does not turn on any particular claim construction for these terms, and because these constructions are not in dispute, we need not determine any specific claim construction for these terms in this proceeding.

4. *Means-plus-function terms*

In our Institution Decision we accepted Petitioner’s proposed constructions for the several “means for” and “code for” limitations recited in claims 15 and 18. *See* Inst. Dec. 42 (The Board explaining that “we find Petitioner’s proposed constructions of these term under 35 U.S.C. § 112(6) consistent with the record in this case.”). These constructions are also consistent with the District Court proceeding. Inst. Dec. 39–43; *see also* Ex. 1012, 1–4. Patent Owner does not address the means-plus-function terms in the challenged claims.

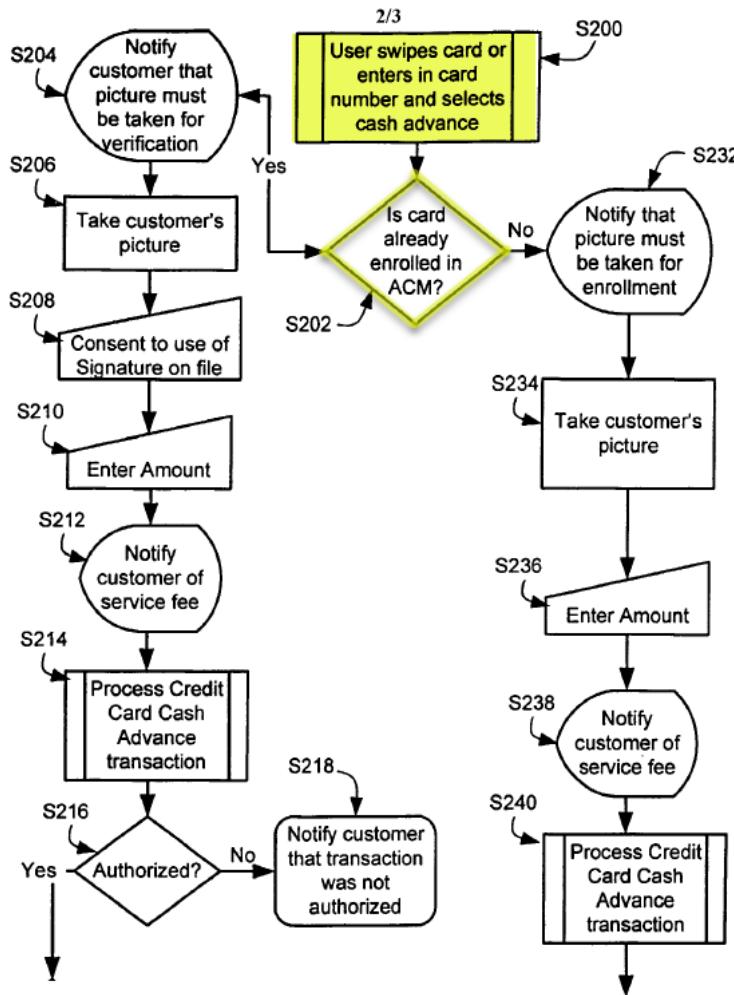
Because patentability on the claims at issue in this case does not turn on construction of the relative structures and functions of these means-plus-function terms, and because they are not in dispute, we maintain the constructions from our Institution Decision including that “code for” is an equivalent recitation for “means for.” Inst. Dec. 39–43.

D. *Ground 1: Claims 3, 4, 6–11, 15, 16, and 18 – Obviousness over Sanford (Ex. 1004) and Hsu (Ex. 1003)*

For the reasons below, and on the complete record before us, Petitioner has shown by a preponderance of the evidence that claims 3, 4, 6–11, 15, 16, and 18 would have been obvious over Sanford and Hsu.

I. *Sanford (Ex. 1004)*

Sanford is titled “Credit Card Transaction without using a Pin with Automated Cashier Machine” and describes “[a]n automated cashier machine (ACM) is provided that offers a secure and convenient way for users to access cash from their card without using a PIN.” Ex. 1004, Abstract, codes (54), (57). Sanford describes that “[b]y verifying a user’s image using facial biometrics, transactions may be conducted without using a pin.” *Id.* ¶ 7. Sanford explains further that “[o]ther methods of verification known in the art may also be used, such as iris, voice signature, and fingerprint technology.” *Id.* ¶ 20. The relevant part of Sanford’s Figure 2, as annotated by the Board, is reproduced below.



IPR2022-01094
Patent 8,620,039 B2

Sanford's figure 2 is a block diagram illustrating a method for performing a PIN-less credit card transaction using an ACM (automated cashier machine). *Id.* ¶ 24. After swiping a user's card at step 200, the system determines whether the user's card information is already stored, i.e. enrolled, and "the ACM 12 determines if the credit card account number of the user is enrolled to use the PIN-less credit card system." *Id.* In determining if the user is enrolled, "ACM 12 may communicate with ACM computer system 18 to look up the user's credit card number." *Id.* ¶ 25. At step 202, highlighted yellow above, ACM 12 determines an enrollment course of action; if the card is not enrolled, moving to step 232, or, if the card is already enrolled, conducting a verification course of action via step 204. *Id.*

2. *Hsu (Ex. 1003)*

Titled "Controlled Access to Doors and Machines Using Fingerprint Matching," Hsu describes "[a] system and related method for controlling access to building doors or to machines, such as automatic teller machines (ATMs)." Ex. 1003, Abstract, codes (54), (57). Hsu describes using "an account number or employee number, to access a fingerprint database (44) and retrieve reference fingerprint data previously stored there during an enrollment procedure." *Id.*, Abstract. Figure 3 from Hsu is reproduced below.

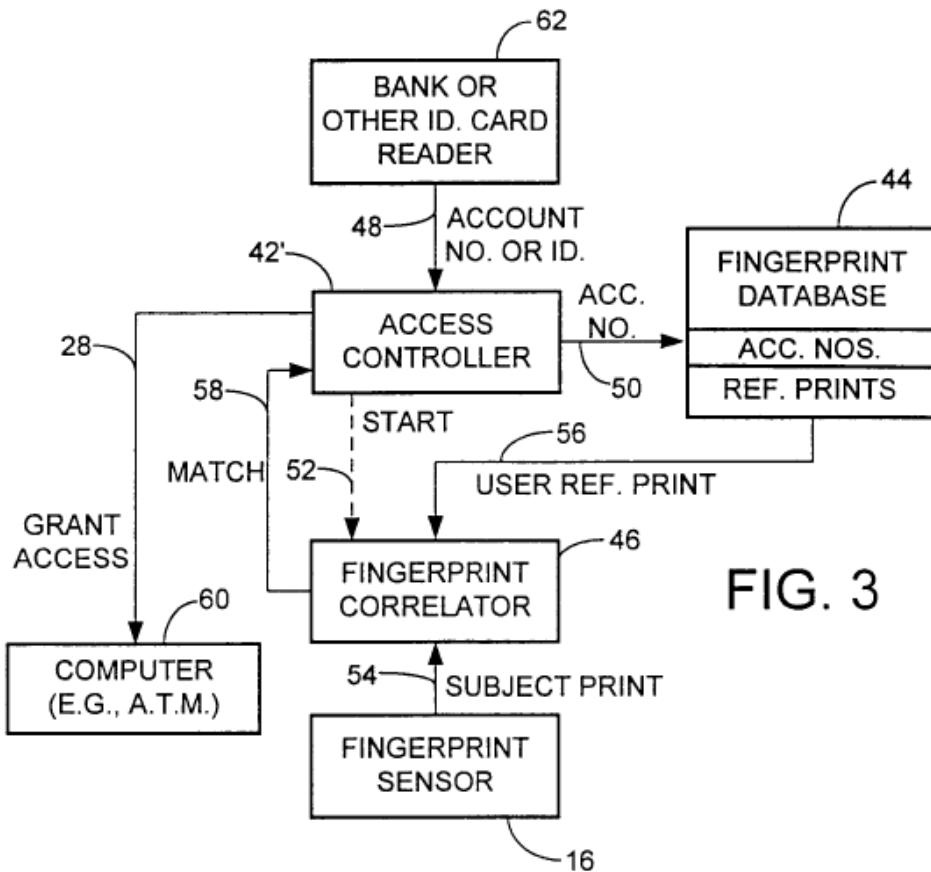


FIG. 3

Hsu's Figure 3 is a block diagram illustrating card reader 62 reading "an account number or other type of identification unique to the user, and passes this data to the access controller 42' over line 48." *Id.* at 6:10–12. Based on the user's unique identification access controller 42' communicates with finger print database 44 "to access the fingerprint database 44 and obtain a user reference fingerprint on line 56 from the database." *Id.* at 6:14–16. Hsu explains that

[t]he controller 42' also sends a "start" signal on line 58 to the fingerprint correlator 46, which compares the reference fingerprint with a subject fingerprint image supplied from the sensor 16 over line 54. If the correlator 46 finds a match, the correlator sends a signal over line 58 to the access controller 42', which transmits an appropriate signal to the computer 60 on line 28, indicating that access has been granted.

Id. at 6:16–24.

Hsu also describes an enrollment process shown in Figure 4 and reproduced below.

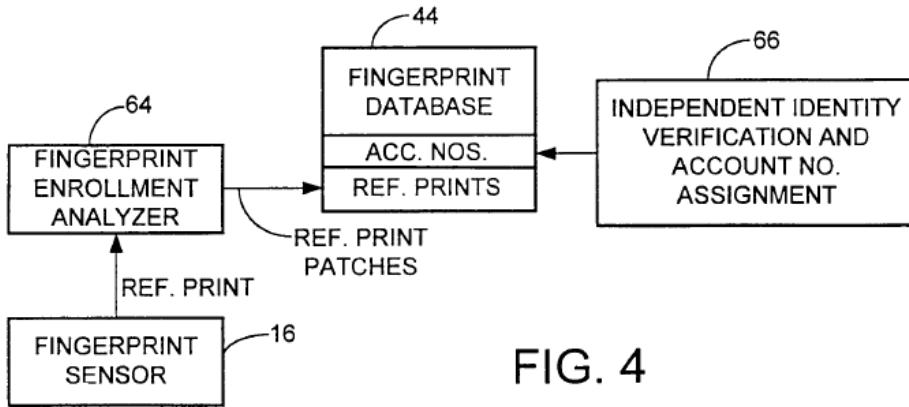


FIG. 4

Hsu's Figure 4 illustrates a block diagram showing that a user's fingerprint is obtained by fingerprint sensor 16 and passes through fingerprint enrollment analyzer 64 before being stored in fingerprint database 44. *Id.* at 7:51–8:23. Hsu explains that along with providing a fingerprint during enrollment, “[a]t the same time, the user's identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the user also presents an account number, employee number or similar identity number.” *Id.*

3. *Independent claim 3*

We consider initially the elements of independent claim 3.

a) *Petitioner's Arguments*

- (1) 3[P] – “A method of securing a process at a verification station”

Petitioner argues that Sanford discloses a “method of securing a process at a verification station” because Sanford teaches that a user needs to be verified at an ATM, e.g., Sanford's ACM (automated cashier machine). Pet. 13 (citing 1006 ¶¶ 268–272). Specifically, Sanford discloses a secure

IPR2022-01094
Patent 8,620,039 B2

and easy way for a user to access cash using a picture, i.e., facial recognition, and without having to use a PIN. *Id.* (citing Ex. 1006 ¶ 269).

Sanford illustrates an exemplary verification system in Figure 1, reproduced below, as annotated by Petitioner (*id.* at 14).

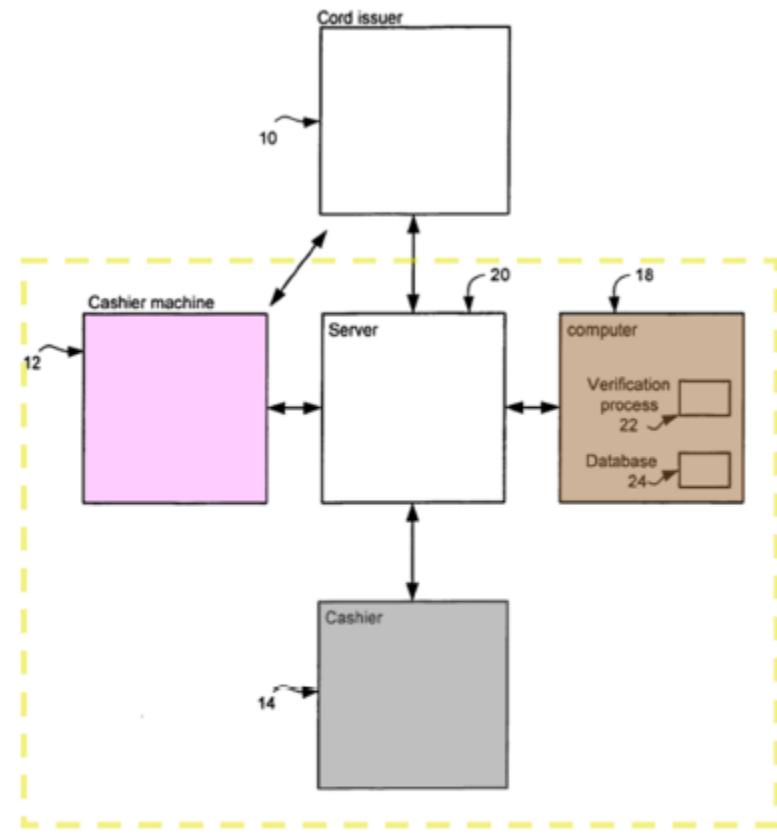


Fig. 1

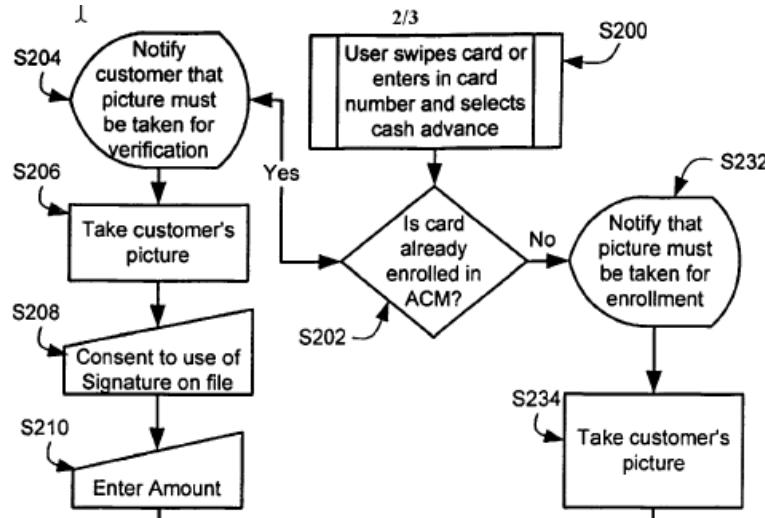
Figure 1 of Sanford illustrates verification system 10 including cashier machine 12 “capable of taking a picture of a person, and dispensing money” and server 20 “capable of receiving and forwarding communications to and from components of system 10.” Ex. 1004 ¶¶ 16–17. Sanford explains that “[v]erification process 22 also may query database 24 to validate a user’s credit card number associated with the picture to a card number associated

IPR2022-01094
Patent 8,620,039 B2

with the user's picture in the database. Additionally, verification process 22 may query database 24 to verify other aspects of identifying information in the profile." *Id.* ¶ 21.

(2) 3[A] – "(a) providing card information from a card device to a card reader in the verification station;"

For limitation 3(a), Petitioner argues that Sanford's Figure 2 and step 200 disclose swiping or inserting a card in a card reader. Pet. 17–18 (citing Ex. 1004 ¶ 24, Fig. 2). According to Petitioner, Sanford teaches a process including providing *information* from a card to a card reader at a verification station, e.g., Sanford's ACM 12. *Id.* at 17. An excerpt from Sanford's Figure 2 is reproduced below.



Sanford's Figure 2 illustrates step 200 (S200) for swiping or entering a card number at a verification station, and step 202 (S202) determines whether the card is already enrolled.

(3) 3[B] – “(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station”

Petitioner argues that Sanford’s Figure 2, step 234, which states “[t]ake customer’s picture,” teaches inputting a biometric signature, in the form of a user’s picture, to a biometric reader in the ACM verification system. Pet. 18–19 (citing Ex. 1004 ¶ 16). Mr. Lipoff testifies that a person of ordinary skill in the art “would have understood that if a fingerprint biometric were used in Sanford’s system, then the picture taking device would be replaced with a fingerprint reader.” Ex. 1006 ¶ 279.

(4) 3[C] – “(c) determining if the provided card information has been previously provided to the verification station;”

Petitioner contends that Sanford teaches this limitation because at step 202, as shown in Figure 2, Sanford determines whether the card is enrolled, i.e., stored in memory. Pet. 21 (citing Ex. 1004, Fig. 2, step 202; Ex. 1006 ¶¶ 282–285). Mr. Lipoff testifies that a person of ordinary skill in the art would have understood that this “means determining if the card has been previously enrolled, which Sanford discloses,” because “after a user provides the credit card account number at step S200 (blue), ‘ACM 12 determines [at step S202 (yellow)] if the credit card account number of the user is enrolled to use the PIN-less credit card system.’” Ex. 1006 ¶ 283 (quoting Ex. 1004 ¶¶ 24–25).

(5) $3[D(P)+D(1)+D(2)] -$ “*(d) if the provided card information has not been previously provided to the verification station;*

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;”

Petitioner argues that Sanford checks to see if card information has, or has *not*, been provided, i.e., enrolled, as outlined in Figure 2, step 202; if the card has *not* been enrolled, Sanford then stores the user’s picture or, for example, other biometric data, such as a fingerprint. Pet. 23–24 (citing Ex. 1004 ¶ 25). Petitioner explains, however, that “Sanford does not provide specific details about how the user’s picture or fingerprint is stored in the database.” *Id.* at 27 (citing Ex. 1004 ¶¶ 21, 18). Petitioner argues that Hsu discloses a database that creates an association between a biometric fingerprint and a user employee number or account number. Pet. 33 (citing Ex. 1003 ¶¶ 26, 20). Mr. Lipoff testifies that a person of ordinary skill in the art “would have known that Sanford’s database could be setup like that disclosed in Hsu to store Sanford’s credit card numbers and associated pictures/fingerprints . . . such that given a user’s credit card number, Sanford’s ACM could locate the customer’s picture/fingerprint data at the associated memory location.” Ex. 1006 ¶ 292. Mr. Lipoff testifies further that a person of ordinary skill in the art “would have understood that the biometric signature (e.g., fingerprint) in the Sanford-Hsu system is not stored at *any* memory location in the database—rather, it is stored at *the* memory location associated with the corresponding credit card number (Hsu’s user/account/employee number) received from a card.” *Id.* ¶ 293

IPR2022-01094
Patent 8,620,039 B2

(citing Ex. 1003 ¶¶ 26, 20). Given the knowledge of a person of ordinary skill in the art regarding how a database and tables relate stored information, Petitioner argues that “the ‘memory location’ for storing the biometric signature (e.g., fingerprint) the Sanford-Hsu system is ‘defined by the provided card information.’” Pet. 28 (citing Ex. 1006 ¶ 293).

Petitioner points out that Hsu’s Figure 4, as shown below and annotated by Petitioner (*id.* at 72), depicts memory and storage 44 where an account number is stored in the database associated with a fingerprint. *Id.*

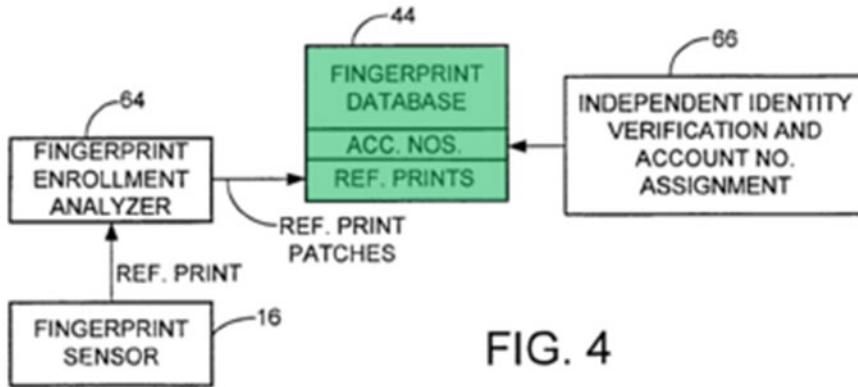


FIG. 4

Hsu’s Figure 4 is a block diagram illustrating storage 44 (highlighted green) including “fingerprint database,” “Acc[ount] Nos.,” and “Ref. Prints.” Ex. 1003, 6:51–58.

(6) *3[E(P)+E(I)] – “(e) if the provided card information has been previously provided to the verification station;*

(ea) comparing the inputted biometric information to the biometric signature stored in the memory at the memory location defined by the provided card information”

In line with its analysis of the above limitations, Petitioner contends that Sanford discloses checking if the card information has or has not been provided, i.e., enrolled, and if it has been, then the verification process can

IPR2022-01094
Patent 8,620,039 B2

compare the picture or fingerprint stored in the manner of Hsu’s database; for example, with a user’s provided picture or fingerprint. Pet. 31 (citing Ex. 1006 ¶¶ 300–302). In this case, in which Sanford discloses that a user is enrolled, Mr. Lipoff testifies that “[t]he ‘verification process 22 may employ an algorithm based on facial biometrics’ and compares the inputted image to a stored picture/fingerprint.” Ex. 1006 ¶ 301 (quoting Ex. 1004 ¶ 19).

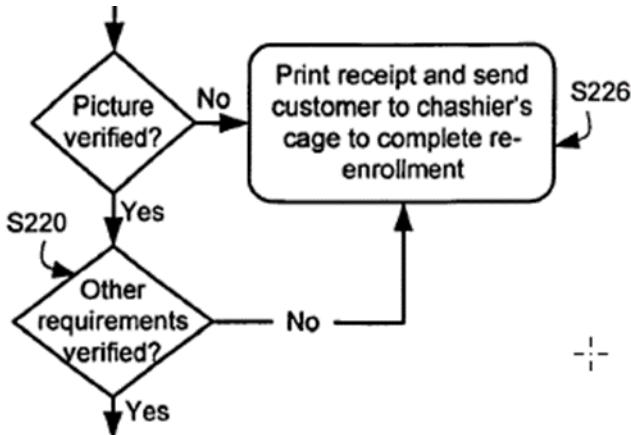
(7) *3[E(2)] – “(eb) if the biometric signature matches the stored biometric signature, performing the process dependent upon the received card information”*

Petitioner argues that Sanford teaches this limitation because Sanford verifies the user, for example, in Fig. 2, steps 204–220, which illustrate that a user’s picture or other biometric signature, such as a fingerprint, is compared and verified, in the manner taught by Hsu’s database for example, with a user’s stored picture or fingerprint. Pet. 33. Mr. Lipoff testifies that after verification Sanford discloses “performing the process [e.g., antecedent process from the preamble, here Sanford’s cash dispensing] dependent upon the received card information [e.g., Sanford’s credit card account number].” Ex. 1006 ¶ 305. In other words, according to Petitioner and Mr. Lipoff, Sanford’s process is carried out—that is dispensing cash—after successfully comparing the biometric signatures, and a badge or card account number, for example as described by Hsu, points to the location of the stored biometric signature for verification and comparison purposes.

(8) *3[E(3)] – “(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.”*

According to Petitioner, Sanford teaches that if the biometric signature does not match a stored signature, then, as shown and described in

Figure 2, step 226, the user is printed a receipt and instructed to re-enroll, and the system does not dispense cash to the user. Pet. 34–35 (citing Ex. 1004 ¶ 30). An excerpt from Sanford’s Figure 2 is reproduced below.



Sanford’s Figure 2 describes at step 226 (S226) that where a user’s picture cannot be verified, “[p]rint receipt and send customer to c[]ashier’s cage to complete re-enrollment.”

(9) *Analogous Art and Motivation to Combine Sanford and Hsu*

Petitioner argues that Sanford and Hsu are analogous prior art with respect to the ’039 patent. Pet. 37. Petitioner contends that “[b]oth references (and the ’039 Patent) are directed to ways of performing efficient biometric authentication, including using fingerprints.” *Id.* Petitioner argues that “[b]oth references (and the ’039 Patent) teach authenticating a user by comparing a fingerprint captured by a sensor to a stored fingerprint.” *Id.* (citing Ex. 1003, Abstract; Ex. 1004, Abstract).

We consider two criteria when evaluating whether prior art is analogous: (1) whether the art is from the same field of endeavor, regardless of the problem addressed; and (2) if the reference is not within the field of the inventor’s endeavor, whether the reference still is reasonably pertinent to

IPR2022-01094
Patent 8,620,039 B2

the particular problem with which the inventor is involved. *In re Clay*, 966 F.2d 656, 658–59 (Fed. Cir. 1992).

The '039 patent is directed broadly to “security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs.” Ex. 1001, 1:14–16. More specifically, the '039 patent explains that its disclosure addresses “problems relating to secure access and/or secure processes, by automatically storing a card user’s biometric signature in a local memory in a verification station comprising a card reader, [and] a biometric signature reader.” *Id.* at 2:53–57. Based on framework and disclosure, we determine that a reasonable field of endeavor involves enrollment and user verification systems including card devices and biometric signatures.

As Petitioner points out, both Sanford and Hsu expressly disclose enrollment and biometric user verification systems that compare a user fingerprint to a stored fingerprint for identity verification purposes.

See, e.g., Ex. 1003 ¶¶ 4, 13, 20, 24, Fig. 3; *see also* Ex. 1004 ¶¶ 4, 8–9, 16, 36. For example, Hsu explains that “FIG. 2 shows the principal components of the access control unit 14 in block diagram form, including an identification polling transceiver 40, a door controller 42, a fingerprint database 44, and a fingerprint correlator 46.” *Id.* at ¶20. Similarly, Sanford describes that in “a secure and convenient way for users to access cash from their card without using a PIN . . . [a]n identifying image of a user is taken and an amount for withdraw is received. If the amount for withdrawal is approved, the ACM verifies the identifying image of the user to an image of the user in a profile.” Ex. 1004 ¶6. Also, Sanford states that “[o]ther methods of verification known in the art may also be used, such as iris, voice signature, and fingerprint technology.” *Id.* ¶20.

On the complete record now before us, we are persuaded that Sanford and Hsu are analogous art to the '039 patent as they are directed to the same field of endeavor, which is—enrollment and user verification systems including card reading devices and biometric signatures.

With respect to motivation to combine, Petitioner argues that although Sanford does not expressly disclose “a specific memory structure with a memory location for storing a picture/fingerprint that is defined by card information[,] [t]his is disclosed by Hsu.” Pet. 37. To this end, Petitioner argues that

[b]oth references (and the '039 Patent) teach that the stored fingerprint is associated with a number provided by the user and/or the user's card. Sanford discloses a user's picture (or fingerprint) associated with a user's card number provided by a user. Hsu discloses that the stored fingerprint data is associated with a user number or account number provided by a user's card.

Id. (citing Ex 1003 ¶¶ 18–21, 26).

Petitioner's declarant, Mr. Lipoff, testifies that a person of ordinary skill in the art would have implemented Hsu's database 44 in Sanford's system because “Hsu discloses that '[t]he database is basically a table that associates each user number with a stored fingerprint image, or with selected distinctive attributes or features of the user's fingerprint image.’” Ex. 1006 ¶ 311 (quoting Ex. 1003 ¶ 20, Fig. 4). Mr. Lipoff reasons that combining the references “improve[s] the efficiency of a biometric authentication system by comparing a captured fingerprint with a single stored fingerprint in a one-to-one manner, instead of needing to compare against multiple stored fingerprints in a one-to-many manner.” *Id.* ¶ 310.

On this record, we find persuasive Petitioner's explanations for a motivation to combine Sanford and Hsu. Hsu, as Mr. Lipoff testifies

IPR2022-01094
Patent 8,620,039 B2

persuasively, describes specifically *how* a person of ordinary skill in the art would implement a database in a verification system to associate an account or credit card number with a stored biometric signature. *Id.* ¶¶ 281–294. In addition, Mr. Lipoff provides persuasive reasoning as to why a person of ordinary skill in the art would have looked to Hsu to “perform a database look-up to locate the user’s biometric data, including picture/fingerprint and other data, at the specific memory location defined by the card/user number” *Id.* ¶ 313; *see also* KSR, 550 U.S. at 420 (explaining that “any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed”).

b) Patent Owner’s Arguments

Patent Owner focuses its arguments on limitation 3[C(P)] and 3[C](1), arguing that “Hsu is devoid of any teaching or suggestion that the user’s card information sets or establishes (*i.e.*, defines) the memory location for the user’s fingerprint data during enrollment.” PO Resp. 11 (citing Ex. 2039 ¶ 46). According to Patent Owner, Hsu does not “set” or “establish” a memory location for the fingerprint data because Hsu mainly describes that “[t]he account number is stored in the database 44 in association with the user’s fingerprint image data.” *Id.* at 12 (quoting Ex. 1003, 7:1–12). Patent Owner’s position is that Hsu does not define any memory location in particular, but “that the user’s fingerprint data and account number are presented *at the same time* and are then stored in the database *in association with* each other.” *Id.* at 13 (citing Ex. 2039 ¶ 49). In other words, Patent Owner’s argument is that, unlike the claimed method, Hsu’s card information does not provide data that sets or establishes *where*,

i.e., at what memory location or address, the system will *store* the fingerprint data.

c) Analysis

Hsu expressly describes an enrollment process for a user including fingerprint database 44 and describes that “the fingerprint database 44 contains reference fingerprint image data for each user, employee, or customer using the system, and that the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers.” Ex. 1003 ¶ 26. Hsu’s Figure 4, illustrating the enrollment process, as annotated by Petitioner (Pet. 72), is reproduced below.

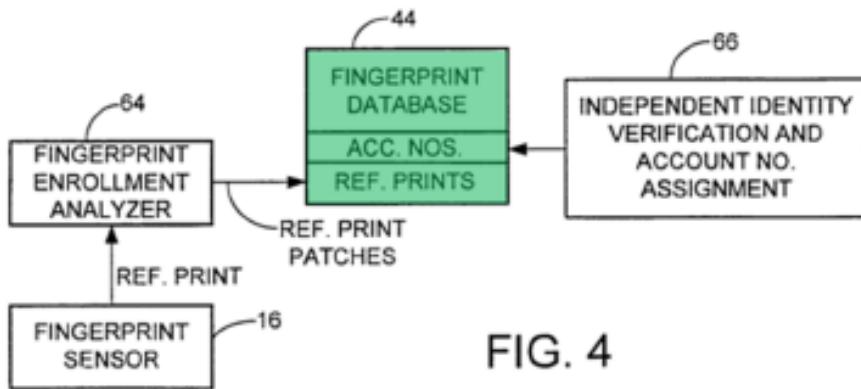


FIG. 4

Hsu’s Figure 4 is a block diagram showing an enrollment process illustrating fingerprint database 44 (highlighted green) including reference prints and related account number for each user or employee. Ex. 1003 ¶ 26.

Based on the description and Figure 4, Hsu tells us a location, that is *where*, i.e., in fingerprint database 44, the fingerprint is to be stored during enrollment. Hsu explains that in the fingerprint database 44 “fingerprint data are associated with corresponding user numbers, or employee or customer account numbers.” *Id.* Accordingly, we understand from this

IPR2022-01094
Patent 8,620,039 B2

description that the user’s fingerprint is stored in relation to, i.e., “associated with,” the user’s employee account number, for example. Still, a key question is *how* is the fingerprint data stored during enrollment. Consistent with our claim construction, the card information must “set” or “establish” where the fingerprint data is to be stored—that is, the location must be “*contingent upon or determined by* the user’s account number itself during enrollment.” *See supra*, Section II.C.2. Petitioner relies on Hsu for this teaching, Pet. 28–32. Hsu explains that when a user presents a fingerprint during enrollment “[a]t the same time, the user’s identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the user also presents an account number, employee number or similar identity number.” Ex. 1003, 7:4–8. In this way, Hsu describes presenting identification data apart from biometric data, and includes presenting, for example, an employee identification card or badge, including the user’s employee number. *See* Ex. 1003 ¶11 (describing that “the identification medium carried by each user includes a machine-readable card, and the step of reading data from an identification medium includes reading data from a card reader in which the machine-readable card is placed by the user”). Understanding that during enrollment Hsu stores the user’s fingerprint data “associated with” a user’s employee number on the card, we further understand that the identification information, e.g., employee number, on the identification card defines, sets, or establishes, *where* the fingerprint is stored; that is—the user’s fingerprint data is stored with the database record corresponding to the relevant employee number.

Given this, we conclude that Patent Owner’s position that Hsu does not disclose a memory location “defined by,” “set,” or “established” by card

IPR2022-01094
Patent 8,620,039 B2

information is not accurate. *See* PO Resp. 12 (arguing that “[t]here is definitively no teaching or suggestion that the user’s account number (or similar identity number) sets or establishes the memory location for the fingerprint data during enrollment”) (citing Ex. 2039 ¶ 48). Patent Owner’s argument mainly contrasts the term “associated with,” as described in Hsu, with our claim construction that “defined by” means “set” or “established.” *Id.* We agree that these are different words, but an ordinary meaning of “associated” is “related, connected, or combined together.” MERRIAM WEBSTER ONLINE DICTIONARY, <https://www.merriam-webster.com/dictionary/associated> (last visited Jan. 9, 2024) (Ex. 3001). Considering common database structures and functions, we are persuaded that Hsu, by “associating” a user’s fingerprint data with a database record corresponding to a particular employee, concomitantly discloses “defining,” “setting,” or “establishing” a memory location for the fingerprint data in relation to the employee account number. Consistent with our understanding of Hsu’s disclosure, Mr. Lipoff testifies persuasively that in Hsu “[t]he ‘fingerprint image, or [] selected distinctive attributes or features of the user’s fingerprint image’ are not stored at *any* memory location in the database—rather, it is stored at a memory location associated with the specific user/employee number received from a card.” Ex. 1006 ¶ 93 (citing Ex. 1003 ¶ 26).

Patent Owner’s counsel made clear, during oral argument, its position that “there’s no discussion at all in Hsu that the ID number/card information in enrollment for purposes of storing the signature, stores [fingerprint data] at a specified location -- by location specifically specified by the card data.” Tr. 42:21–23. But we do not agree with this position. As discussed above, Hsu describes that fingerprint data is stored associated with the card data,

IPR2022-01094
Patent 8,620,039 B2

e.g., an account or employee number. Ex. 1003 ¶ 26 (describing that “the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers”). Consistent with our claim construction, the “association” is the *where*. In other words, we understand that Hsu’s associating the fingerprint data with the personal data record in fingerprint database 44 defines, sets, or establishes where the fingerprint data is stored. This occurs, as Hsu explains, because during enrollment the user data such as account or employee number is supplied by the user’s card. *See id.* (explaining that during enrollment, in addition to a fingerprint image, “the user also presents an account number, employee number or similar identity number”). We do not consider it a significant leap, or even a leap at all, to understand that associating the fingerprint data according to, that is—“contingent on, or determined by,” the user’s account number or employee number on Hsu’s card or badge, sets or establishes the database record or address location *where* the fingerprint data is stored in Hsu’s fingerprint database 44.

Patent Owner also argues that “[i]n contrast to the claimed method, Hsu teaches that the user’s fingerprint data and account number are presented *at the same time* and are then stored in the database *in association with* each other.” PO Resp. 13 (citing Ex. 2039 ¶ 49). Patent Owner’s declarant, Dr. Russ, similarly testifies that “in Hsu, the fingerprint data and the account number are presented together and are then stored together . . . [t]here is no step in Hsu wherein the account number (or the ‘card information’) first sets or establishes the memory location.” Ex. 2039 ¶ 49. This argument takes advantage of the fact that Hsu does explicitly state a temporal order for “storing . . . the biometric signature” as recited in claim 1. However, as we explained in our claim construction,

IPR2022-01094
Patent 8,620,039 B2

during an enrollment process the claimed “biometric signature,” e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been “defined,” as in “set” or “established,” in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint is received during enrollment, the card information provides data that establishes *where*, i.e., at what memory location or address, the system will *store* the fingerprint data.

Section II.C.2. Similarly, in Hsu, the fingerprint data can only be stored once the system has received data indicative of, for instance, an employee number from a user’s identification badge, which thus defines a database record with which the fingerprint data can be “associated.”

This all makes sense, logically, because Hsu’s fingerprint data are not randomly stored, as Mr. Lipoff explains, “in *any* memory location.”

Ex. 1006 ¶ 93. Hsu’s fingerprint data cannot be stored until directed to, i.e. “associated with,” a certain database address or record, and in Hsu that is a database record containing the user’s identification information.

See Ex. 1003, 7:7–12 (describing that during enrollment “the user also presents an account number, employee number or similar identity number . . . [t]he account number is stored in the database 44 in association with the user’s fingerprint image data”). Accordingly, from a temporal standpoint during enrollment, Hsu must also use card information, e.g., an employee number, to define, set, or establish a memory location with which the fingerprint data can be associated, before storing the fingerprint data.

Commensurate with our understanding of Hsu’s disclosure, we credit Mr. Lipoff’s testimony that even though Hsu does not explain exactly “how a new user record is created” during enrollment, a person of ordinary skill in the art would have “tried] using simple known options for creating database records.” Ex. 1032 ¶ 32. Mr. Lipoff explains persuasively that “upon a user

IPR2022-01094
Patent 8,620,039 B2

enrolling, they provide a previously unseen card/user number, [and] the system then creates a new record for the user, including setting/establishing for the first time the memory location for storing the user's fingerprint." *Id.* ¶ 33.

When asked during his deposition to describe Hsu's database structure and functions, Mr. Lipoff testified consistently with his declaration, explaining essentially that it is the user's employee or account number that defines where the fingerprint data is stored:

Q. So the account number indicates where the fingerprint is stored because they are stored in association with each other; is that correct?

...

A. THE WITNESS: Well, I think it's – it's more than that. The structure that the database, as Hsu describes it, I believe -- let me see. I think it's in paragraph 20. Let me see if I can find it. Yeah, so in paragraph 20, column 4, the database is basically a table that associates each user number with a stored fingerprint image or selected attributes.

So what this is telling me is the user number, which you -- you said we should call the account number, I believe it's the same thing here, is -- is a database, and so the user number is defining the memory location in which the stored fingerprint image will be stored because the structure of the database is one, as indicated here in column 4, that starts with the user number telling you where to find the memory location that has the stored fingerprint image.

Ex. 1041, 33:16–34:9. When Patent Owner's counsel pointed out that Hsu's paragraph 20 did not pertain specifically to enrollment, Mr. Lipoff explained that the database structure and function in paragraph 20 also applies to the enrollment process shown in Figure 4:

A. Paragraph 20 describes the principle [sic] components of the access control unit, which includes the fingerprint database

which is the same fingerprint database that's in – that's in – I'm sorry. Same fingerprint database that's in Figure 4. Figure 4 is the previous paragraph of Hsu we were discussing. Paragraph 26 is the enrollment procedure, but by the time you get to the enrollment procedure, Hsu, earlier in paragraph 20, defined the structure of that same database -- database item 44 in Figure 4.

Id. at 34:19–35:9.

Summarizing its position, Patent Owner argues that “Hsu merely discloses that the user’s account number and fingerprint data are stored in association with each other. Hsu offers no other teachings as to how the account number and fingerprint data are stored in the database.” PO Resp. 15 (citing Ex. 2039 ¶¶ 53–54). Considering our analysis and the evidence discussed above, we disagree. We are persuaded that Hsu does, in fact, explain *how* the account number and fingerprint data are stored in the fingerprint database. Hsu establishes a memory location for storing the fingerprint data in “association” with an employee or account number, and the “association” is contingent on receiving the employee or account number from Hsu’s card or badge during enrollment. *See* Ex 1003, 7:10–12, Fig. 4 (explaining that “[t]he account number is stored in the database 44 in association with the user’s fingerprint image data”).

Overall, we are persuaded based on Petitioner’s arguments and evidence, including the testimony of Mr. Lipoff, that Hsu’s association of a fingerprint with a user’s underlying account or employee number in a database record during enrollment discloses limitation 3[D](1), namely “storing the inputted biometric signature in a memory at a memory location defined by the provided card information.” Ex. 1001, 12:61–63.

Patent Owner does not present substantive arguments with respect to the remaining limitations 3[P]–[D] and 3[D](2)–[E](3), nor with respect to

IPR2022-01094
Patent 8,620,039 B2

the combination of Sanford and Hsu. *See* PO Resp. 10–15. Having reviewed the entirety of the record now before us, specifically the disclosures in Hsu and Sanford, we accept Petitioner’s arguments and evidence with respect to the remaining limitations as our own. Pet. 12–36. We also find that Petitioner and Mr. Lipoff have provided articulated reasoning with evidentiary underpinning as to why an ordinarily skilled artisan would have been motivated to combine the teachings of Sanford and Hsu. *Id.* at 37–39; Ex. 1006 ¶¶ 108–115.

d) Conclusion as to claim 3

Based on the complete record before us and for the reasons expressed above, we are persuaded that Petitioner has shown by a preponderance of evidence that claim 3 would have been obvious over Sanford and Hsu.

4. Dependent claim 4

Claim 4 depends from claim 3 and recites in part “wherein the card device is one of a card in which the card information is encoded in a magnetic strip;” or alternatively, “a smart card [or] . . . a key fob.” Ex. 1001, 13:12–21.

Patent Owner does not provide separate, substantive arguments with respect to claim 4, but mainly argues that claim 4 “contain[s] the ‘memory location defined by the provided card information’ limitation examined above.” PO Resp. 24. Patent Owner then contends, “As the prior art cited by Petitioners does not teach this limitation, the cited prior art does not render these dependent claims obvious as a result thereof.” *Id.*

Petitioner argues that “Sanford also discloses that this card information is encoded in a magnetic strip.” Pet. 40 (citing Ex. 1004 ¶¶ 16, 40). Petitioner also argues that Hsu discloses each of the specific cards and key fobs recited in dependent claim 4. *Id.* at 40–41 (citing Ex. 1003 ¶¶ 7,

IPR2022-01094
Patent 8,620,039 B2

24). We find Petitioner's evidence persuasive; for example, Hsu describes that “[t]he card may be encoded with data using a magnetic stripe, bar codes, or any other means. Alternatively, the card may be a ‘smart card’ that includes an electronically readable memory.” Ex. 1003, 6:5–9. For dependent claim 4 we have considered and on the complete record before us, in addition to our analysis above, accept as our own, Petitioner's arguments and evidence set forth at pages 40–41 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 2 would have been obvious over Hsu and Sanford.

5. *Dependent claim 6*

Claim 6 also depends from claim 3 and recites “wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station.” Ex. 1001, 13:28–31.

Patent Owner does not provide substantive arguments with respect to claim 6, but mainly argues that claim 6 “contain[s] the ‘memory location defined by the provided card information’ limitation examined above.” PO Resp. 24. Patent Owner then contends, “As the prior art cited by Petitioners does not teach this limitation, the cited prior art does not render these dependent claims obvious as a result thereof.” *Id.*

Petitioner points, *inter alia*, to Sanford's disclosure in Figure 1 that illustrates the cashier machine 12 (verification station) communicating with a card issuer, the card issuer ostensibly being financial institution 16 described in Sanford's specification. Pet. 42–43. With respect to “outputting . . . card information,” Mr. Lipoff testifies that a person of ordinary skill in the art “would have understood that when dispensing cash for a user, the user's credit card account number is sent to financial

IPR2022-01094
Patent 8,620,039 B2

institution 16 (or at least doing so would be obvious).” Ex. 1006 ¶ 324. Mr. Lipoff explains, for example, considering Sanford’s Figure 2 as annotated by Mr. Lipoff (Ex. 1003 ¶ 323) and reproduced below, that “if it is determined at step S202 (yellow) that a card is not enrolled, ‘[i]n step S240 [purple], the transaction is sent for pre-authorization to the financial institution . . . , which may use an Address Verification System (AVS) to help validate the users address.’” *Id.* ¶ 323 (quoting Ex. 1004 ¶ 34).

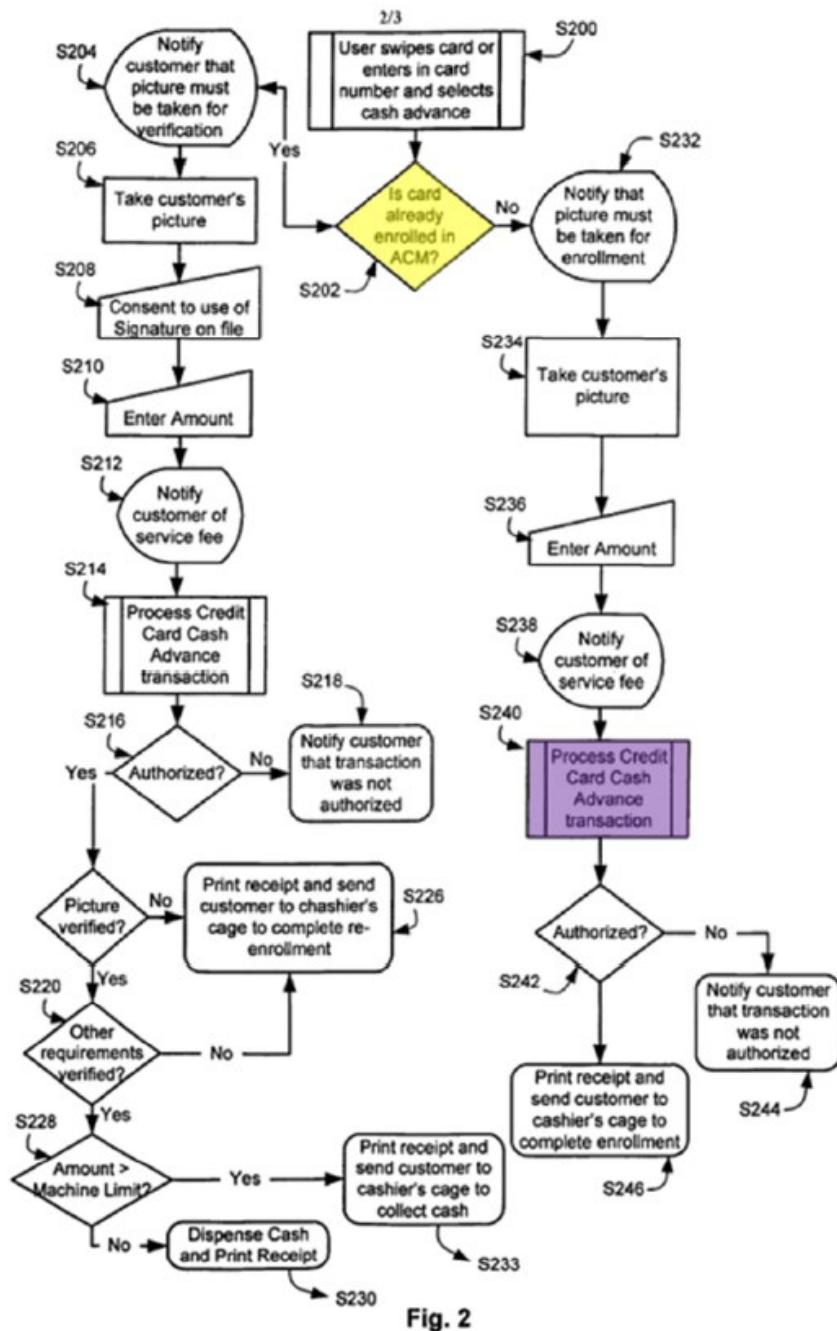


Figure 2 of Sanford illustrates a method for conducting PIN-less credit card transaction in a flow diagram. Ex. 1004 ¶ 24. Mr. Lipoff testifies further that a person of ordinary skill in the art “would have expected that the ‘transaction’ that is sent to the ‘financial institution’ would include the credit card account number.” *Id.*

Mr. Lipoff's testimony as to claim 6 is unrebutted on this record. For dependent claim 6, we have considered and on the complete record before us, in addition to our analysis above, accept as our own, Petitioner's arguments and evidence set forth at pages 41–44 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 6 would have been obvious over Hsu and Sanford.

6. *Dependent claims 7–11*

Claims 7–11 depend directly or indirectly from independent claim 3. Just as for claims 4 and 6, Patent Owner does not provide separate, substantive arguments with respect to dependent claims 7–11, but argues again that these dependent claims "contain the 'memory location defined by the provided card information' limitation examined above. As the prior art cited by Petitioners does not teach this limitation, the cited prior art does not render these dependent claims obvious as a result thereof." PO Resp. 24.

Mr. Lipoff's testimony as to dependent claims 7–11 is unrebutted on this record. For dependent claims 7–11, we have considered and on the complete record before us, in addition to our analysis above, accept as our own, Petitioner's arguments and evidence set forth at pages 44–54 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claims 7–11 would have been obvious over Sanford and Hsu.

7. *Claims 15–16 and 18*

Independent claim 15 is an apparatus claim reciting "[a] verification station for securing a process," and includes similar limitations as independent claim 3. Ex. 1001, 14:22. Different from claim 3, claim 15 also recites "a card device reader," "a biometric signature reader," and for

IPR2022-01094
Patent 8,620,039 B2

the remaining limitations recites “means for” along with the same functional language as in limitations 3[C]–[E].

Patent Owner does not provide separate, substantive arguments with respect to claims 15–16 and 18.

Petitioner argues that besides disclosing a verification station including a card reader, “Sanford discloses that its card reader is part of its ACM [automated cashier machine 12], and is therefore coupled to the ACM.” Pet. 54 (citing Ex. 1004 ¶ 16). Petitioner equates Sanford’s “picture taking device” with the claimed “biometric signature reader” arguing that “when the biometric signature is provided to the biometric signature reader, it is also provided to Sanford’s ACM.” *Id.* at 55 (citing Ex. 1006 ¶ 357).

Considering the “means for” limitations in the remainder of the claim, Petitioner points to the requisite function and structure in the prior art, which are consistent with our claim construction (*see supra* Section II.C.4; *see also* Inst. Dec. 39–43). For example, for limitation 15[C], Petitioner explains that the function of this limitation is “determining if the provided card information has been previously provided to the verification station.” Pet. 56. According to Petitioner, the structure is, “processor unit 105 running software process(es) 206; and equivalents thereof.” *Id.*

Petitioner argues that “as explained for Limitation 3[C], Sanford discloses the recited function.” *Id.* (citing Ex. 1006 ¶ 282–285, 361). For the structure, and considering Sanford’s Figure 1 reproduced below as annotated by Petitioner, Petitioner asserts that “Sanford discloses that ACM computer system 18 (brown), which is part of Sanford’s ACM (yellow), ‘includes a processor . . . [which] may be . . . a computer, workstation, mainframe, pocket PC, personal digital assistant, etc.’” *Id.* (quoting Ex. 1004 ¶ 18).

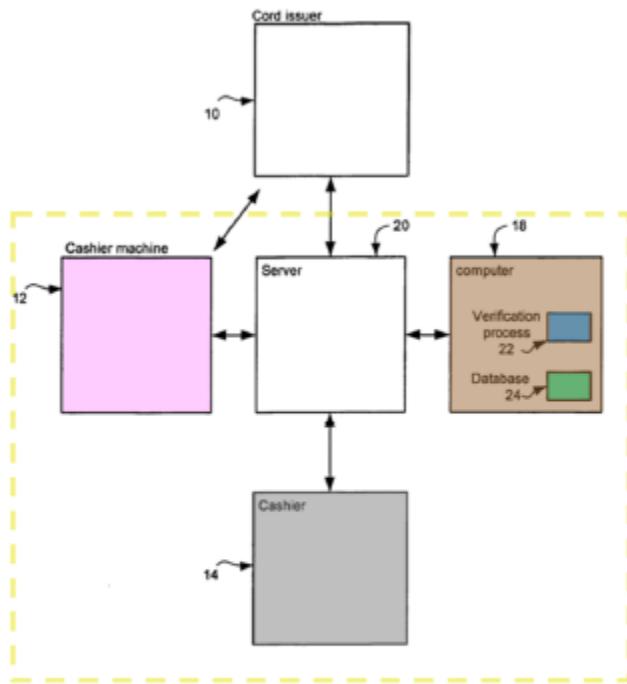


Fig. 1

Sanford's Figure 1, as annotated by Petitioner (Pet. 64), illustrates ACM computer system 18 (brown), encompassing verification process 22 (blue) and database 24 (green). Ex. 1004 ¶ 18. Petitioner points out that Sanford expressly describes that “[t]he processor also preferably includes or is in communication with a verification process 22 [blue] and database 24 [green]. Verification process 22 may be a software- implemented process that communicates with database 24.” Pet. 57 (quoting Ex. 1006 ¶ 18).

Apart from its arguments with respect to independent claim 3[D](1), Patent Owner does not dispute Petitioner's evidence that Sanford, and Sanford in view of Hsu, disclose and teach the limitations of independent claim 15. *See generally* PO Resp. And, in addition to being persuaded that Sanford discloses the necessary structure and function intimated by “means

IPR2022-01094
Patent 8,620,039 B2

for,” we find that Sanford renders obvious limitation 15[C] for the same reasons as limitation 1[C]. Based on our review, we find that the complete record fully supports Petitioner’s showing that the combination of Hsu and Sanford discloses all the limitations of independent claim 15. *See* Pet. 49–56.

Dependent claim 16 is similar to claim 4, and relates to a “verified access system” including, *inter alia*, “a reader for a card in which the card information is encoded in a magnetic strip.” Ex. 1001, 14:51–52. Besides referencing his testimony with respect to claim 4, Mr. Lipoff testifies that similarly “Sanford discloses verification station with card reader and that its ‘card reader may be a magnetic strip reader capable of reading cards with a magnetic strip such as, for example, ATM cards, credit cards, debit cards, or smart cards.’” Ex. 1006 ¶ 387 (quoting Ex. 1004 ¶ 16).

Independent claim 18 includes essentially the same limitations as claim 15, except that the preamble to claim 18 recites:

A non-transitory computer readable medium having recorded thereon a computer program for directing a process or to execute a method for securing a process at a verification station, said program comprising:

Ex. 1001, 14:64–67. And, for example, the limitation of “means for determining if the provided card information has been previously provided to the verification station” in independent claim 15, is recited in independent claim 18 as “code for determining if card information, . . . has been previously provided to the verification station.” *Compare id.* at 14:28–29, *with id.* at 15:1–4. Petitioner asserts that “[t]hese ‘code for’ terms should be construed the same way as ‘means for’ terms (*see* Section VII.B). Thus, for the same reasons discussed for claim 15, Sanford and Hsu disclose or render obvious claim 18.” Pet. 65–66. Mr. Lipoff testifies that “[i]n order for the

IPR2022-01094
Patent 8,620,039 B2

various components of Sanford and Hsu to perform their functions, a POSITA would have understood and found it obvious that both Sanford and Hsu (and the combined system) include one or more processors running computer programs stored on a non-transitory computer readable medium.” Ex. 1006 ¶ 389.

Mr. Lipoff’s testimony as to what a person of ordinary skill in the art would have understood in regards to the known internals, programming instructions, and memory structure for a biometric card enrollment and verification system is unrebutted on this record.

For independent claim 18, Petitioner’s arguments and evidence are in all other respects the same as the arguments and evidence presented with respect to independent claim 15, as Petitioner and Mr. Lipoff specifically refer back to the respective arguments and evidence for the similar limitations in claim 15. Pet. 66.

We have considered, and on the complete record before us, accept as our own, Petitioner’s arguments and evidence set forth at pages 54–66 of the Petition as to claims 15–16 and 18. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claims 15–16 and 18 would have been obvious over Sanford and Hsu.

E. Ground 2: Claims 3, 4, 6–11, 15, 16, and 18 – Obviousness over Sanford, Hsu, and Tsukamura (Ex. 1005)

Because we determine that claims 3, 4, 6–11, 15, 16, and 18 would have been obvious over the combination of Sanford and Hsu, we need not address these same claims as obvious over the combination of Sanford, Hsu, and Tsukamura.

F. *Ground 3: Claim 5 – Obviousness over Sanford, Hsu, and Leu (Ex. 1008)*¹⁴

Dependent claim 5 recites:

A method according to claim 3, wherein:

the card information provided in the step (a) comprises a header and card data; and

the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

Ex. 1001, 13:22–27. Petitioner argues that “Leu discloses a card reader device that reads a card and verifies the card information to determine whether an event (*e.g.*, indicating whether or not the user has achieved a lottery prize”) can be triggered.” Pet. 81 (citing Ex. 1009, 1:26–29; 1:20–27). Figure 3 of Leu, illustrating a card memory, is reproduced below including Petitioner’s annotations (Pet. 82).

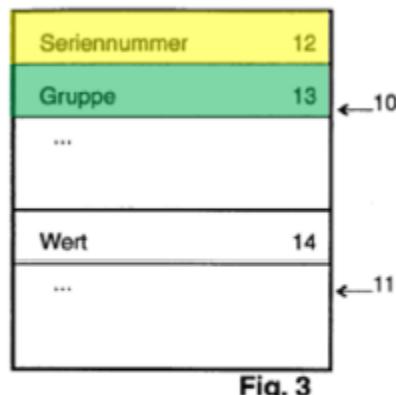


Fig. 3

[Fig. 3 Translation Key:]

12 = serial number

13 = group

14 = value

Leu’s Figure 3 illustrates “the memory of the card” including a non-volatile memory divided into regions 10 and 11. Ex. 1009, 2:5. Leu explains that

¹⁴ Ex. 1009 is the English translation of Ex. 1008.

IPR2022-01094
Patent 8,620,039 B2

“[v]values that can no longer be changed after the card is sold are contained in the region 10, while the data in the region 11 can still be changed.”

Ex. 1009, 3:9–12.

Mr. Lipoff explains that Leu describes a serial number 12 (yellow) different for every card, and “[a] group memory 13 (green) ‘indicates whether a card is a lottery ticket card or a conventional card.’” Ex. 1006 ¶ 423 (quoting Ex. 1009 3:20–22). Mr. Lipoff testifies that “since the group number and the serial number are stored on the card and are to be read by a card reader device . . . , they are both card information.” *Id.* Mr. Lipoff testifies further that in Leu “the determination of whether a card user has won a lottery prize is only performed if the group number indicates that the card belongs to a first set of cards (*i.e.*, lottery cards) and not a second set of cards (*i.e.*, normal prepaid cards).” *Id.* ¶ 426. Thus, according to Mr. Lipoff, “because the card reader is able to interpret the first set of cards (lottery ticket cards) to determine whether a user has won a lottery prize, a POSITA would have understood the first set of cards (lottery ticket cards) are associated with the card reader (verification station).” *Id.*

Petitioner argues that a person of ordinary skill in the art would have combined Leu with Sanford because “Sanford, and Leu are **analogous art** and in the same field of using a card to make transactions. Sanford teaches using a credit card to withdraw cash and Leu teaches using a prepaid card to purchase telephone services.” Pet. 86. Mr. Lipoff testifies that “Leu discloses that the disclosed prepaid cards use the same technology as ‘credit cards,’ which are disclosed in both the ’039 Patent and Sanford.” Ex. 1006 ¶ 249 (citing Ex. 1009, 2:14–29; Ex. 1001, 1:14–16; Ex. 1004, Title). Mr. Lipoff testifies further, that a person of ordinary skill in the art

implementing the Sanford-Hsu (or Sanford-Hsu-Tsukamura) system would have been motivated to perform a preliminary check to determine whether the card being read is a “valid” credit card (*e.g.*, can be interpreted by the card reader and is suitable for cash withdrawal) because, if the system cannot interpret the card or the card is not suitable for cash withdrawal, the system would never dispense money for a card user.

Id. ¶ 430.

Patent Owner does not provide separate, substantive arguments with respect to claim 5 or the motivation and reasons to combine Leu with Sanford and Hsu.

In this proceeding, for claim 5, Petitioner’s arguments and Mr. Lipoff’s testimony are unrebutted. We have considered, and on the complete record before us, accept as our own, Petitioner’s arguments and evidence set forth at pages 80–87 of the Petition as to claim 5. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 5 would have been obvious over Sanford, Hsu, and Leu.

G. Ground 5: Claim 12 – Obviousness over Sanford, Hsu and Houvener (Ex. 1009)

Dependent claim 12 recites:

A method according to claim 3, comprising the further steps of:

(f) storing the card information provided by successive instances of the step (a); and

(g) outputting the information stored in the step (f) for audit purposes.

Ex. 1001, 13:61–66. Petitioner argues that “Houvener discloses ‘stor[ing] the users PIN and the data from the specific transaction as a transaction record.’” Pet. 88 (quoting Ex. 1010, 7:58–60). Petitioner argues that Houvener discloses an audit process where it is described that “if there is

IPR2022-01094
Patent 8,620,039 B2

ever a question as to the voracity of the identification process, the system can recreate a transaction and identify not only the person initiating the transaction but the clerk who was responsible.” *Id.* (quoting Ex. 1010, 7:60–65). Mr. Lipoff testifies that a person of ordinary skill in the art would have “understood that the stored transaction records in Houvener need to include sufficient information to allow the system to ‘recreate a transaction’ and ‘identify . . . the person initiating the transaction.’” Ex. 1006 ¶ 438. Mr. Lipoff testifies that a person of ordinary skill in the art “who looked to further improve the Sanford-Hsu system would have understood that additional fraudulent actions may be uncovered when considering a series of transactions and therefore look for teachings like Houvener.” *Id.* ¶ 441. Including Houvener’s specific transaction data storage and auditing capabilities would be considered, according to Mr. Lipoff, because a person of ordinary skill in the art “would have understood that Sanford discloses the well-known practices of logging card user activities, including card information and biometric information, for auditing purposes” to reduce credit card fraud. *Id.* ¶ 442 (citing Ex. 1004 ¶ 43).

Patent Owner does not provide separate, substantive arguments with respect to claim 12 or the motivation and reasons to combine Houvener with Sanford and Hsu.

In this proceeding, for claim 12, Petitioner’s arguments and Mr. Lipoff’s testimony are unrebutted. We have considered, and on the complete record before us, accept as our own, Petitioner’s arguments and evidence set forth at pages 87–91 of the Petition as to claim 12. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 12 would have been obvious over Sanford, Hsu, and Houvener.

H. Ground 7: Claim 17 – Obviousness over Sanford, Hsu, and McCalley (Ex. 1010)

Dependent claim 17 recites:

A verification station according to claim 15, wherein the memory is incorporated in a tamper-proof manner in the verification station.

Ex. 1001, 14:61–63. Providing an annotated version of McCalley’s Figure 22, reproduced below, Petitioner argues that “McCalley’s ‘overall package may include a tamper resistant housing 191 [yellow] as would be readily understood by those skilled in the art.’” Pet. 92 (quoting Ex. 1011, 10:49–59).

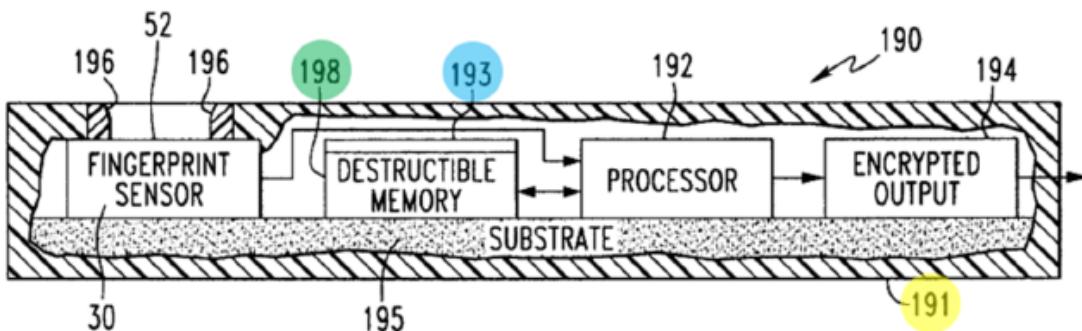


FIG. 22

McCalley’s Figure 22 as annotated by Petitioner (Pet. 92) illustrates in partial cross-section tamper resistant housing 191 encompassing fingerprint sensor 30, memory 198, processor 192, and encrypted output 194. Ex. 1011, 10:45–54. Petitioner argues that “The ’039 Patent, McCalley, Sanford, Hsu and Tsukamura are analogous art and are in the same field of endeavor, *i.e.*, access control using biometric technology. All references (and the ’039 Patent) aim to provide more secured access.” Pet. 93. Mr. Lipoff testifies that “[e]specially in the context of an ATM, as disclosed by Sanford, it was well-known that tamper-proof configuration was beneficial to prevent fraud.” Ex. 1006 ¶ 454. Mr. Lipoff testifies further that a person of ordinary

IPR2022-01094
Patent 8,620,039 B2

skill in the art “would have therefore looked to McCalley for details on how to make the system tamper-proof, such as having a tamper-proof housing.” *Id.* Mr. Lipoff explains that “having a tamper-proof housing and making memories self-destructible, [were] methods commonly in use at the time of the ’039 Patent.” *Id.* ¶455.

Patent Owner does not provide separate, substantive arguments with respect to claim 17 or the motivation and reasons to combine McCalley with Sanford and Hsu.

In this proceeding, for claim 17, Petitioner’s arguments and Mr. Lipoff’s testimony are unrebutted. We have considered, and on the complete record before us, accept as our own, Petitioner’s arguments and evidence set forth at pages 91–94 of the Petition as to claim 17. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 17 would have been obvious over Sanford, Hsu, and McCalley.

I. Grounds 4, 6, and 8: Claims 5, 12, and 17 – Obviousness over Sanford, Hsu, Tsukamura, and one of Leu, Houvener, and McCalley

Because we determine that claims 5, 12, and 17 would have been obvious over Sanford, Hsu, and one of Leu, Houvener or McCalley, we need not address these same claims are obvious over Sanford, Hsu, Tsukamura and one of Leu, Houvener or McCalley.

J. Patent Owner’s Continued 315(b) Arguments

In its Response, Patent Owner reiterates its 315(b) argument that we previously addressed in our Institution Decision. PO Resp. 25–32; Inst. Dec. 10–35. Now, Patent Owner argues that in our prior decision we placed too much weight on a lack of control of the proceedings by Apple, and that

IPR2022-01094
Patent 8,620,039 B2

“[r]ather, a key to the RPI analysis is whether Apple and Petitioners have a structured, preexisting business relationship and whether Apple would receive more than a merely generalized benefit if trial is instituted.” PO Resp. 29–30 (citing *Applications in Internet Time, LLC v. RPX Corp.*, 897 F.3d 1336, 1351 (Fed. Cir. 2018)) (“AIT”).

As an initial matter, we think that Patent Owner’s argument mischaracterizes, or at least oversimplifies, the holding in *AIT*. In *AIT*, the Federal Circuit admonished the Board for (1), making “certain factual findings that are not supported by substantial evidence,” and (2) “fail[ing] to adhere to the expansive formulation of ‘real party in interest’ that is dictated by the language, structure, purpose, and legislative history of § 315(b).” *AIT*, 897 F.3d at 1351. The Federal Circuit explained in *AIT* that the Board failed to appreciate, among other things, the specific nature of the relationship between RPX and Salesforce, “that RPX, . . . is a for-profit company whose clients pay for its portfolio of ‘patent risk solutions.’” *Id.* The Court stated that “the Board did not consider these facts, which, taken together, imply that RPX can and does file IPRs to serve its clients’ financial interests, and that a key reason clients pay RPX is to benefit from this practice in the event they are sued by an NPE.” *Id.* at 1352. As discussed below, we have not overlooked the facts and evidence surrounding the parties’ relationship nor failed to consider the parties’ litigation efforts in the district courts. To the extent Patent Owner has raised valid arguments that may have not been clearly addressed by the Board, we provide the following additional analysis.

With respect to point (1), it is important, factually, that the developer-distributor business relationship between Petitioner and Apple contrasts sharply with the specific intent of the NPE patent portfolio litigation

IPR2022-01094
Patent 8,620,039 B2

relationship between RPX and Salesforce. As we described in our Institution Decision, Petitioner’s product “Yale Smart Locks,” including “the Yale Assure Lock uses a software application (‘App’) on one’s mobile phone, here on an iPhone sold by Apple, to lock and unlock doors. The App is developed by Petitioner, or one of its business partners, and distributed to iPhone users through the Apple App store.” Inst. Dec. 16. The Developer Agreement (the “Agreement”) between Petitioner and Apple mainly provides “a limited license” to use Apple software “to develop and test” the developer’s software applications for integration on Apple’s iOS platforms. Ex. 2009. Importantly, different from *AIT*, in this case we have before us no facts or evidence showing that the intent, express or otherwise, of the Agreement between Petitioner and Apple is *fundamentally* based on protecting one party or the other from patent litigation.¹⁵ To the extent Patent Owner now argues that we did not appreciate all of its arguments and evidence as to the parties’ underlying actions in related district court proceedings, we address that matter in due course below. Before doing so, we turn to point (2), and whether, in this case, our Institution Decision appropriately considered the “expansive formulation of ‘real party in interest.’” *See AIT*, 897 F.3d at 1351.

In *AIT*, the Federal Circuit explained that the “Board’s determination that Salesforce was not a real party in interest under § 315(b) relied on an impermissibly narrow understanding of the common-law meaning of the

¹⁵ We acknowledge that the Agreement contains representations and warranties of noninfringement, as well as indemnification clauses. Ex. 2009, 16, 41–43. We consider that these clauses are perhaps best understood, at least from Apple’s perspective as a distributor, as mechanisms to avoid liability should the need arise, rather than tools exerting control or perpetuating an agency relationship with Petitioner.

IPR2022-01094
Patent 8,620,039 B2

term.” *Id.* at 1357. For one thing, the Court pointed out that “an agent with an ownership interest in the subject matter of the suit, or one who is the trustee of an express trust or a party in whose name a contract has been made for the benefit of another, may qualify as a real party in interest.” *Id.* In this proceeding, Patent Owner has failed to point to any persuasive evidence, apart from software compatibility with Apple’s iOS platforms as discussed in the Agreement, that Apple has any overt interest, influence, development or design influence over Petitioner’s “Yale Smart Locks” products or App. In addition, Patent Owner has produced no evidence that Apple holds any ownership interest, assets, or expressly administers any property rights as a trustee or agent for the benefit of Petitioner indicative of real party in interest relationships under common law.

Essentially the entirety of the evidence of the business relationship in this proceeding is contained within the Agreement, which we already discussed in detail in our Institution Decision. Inst. Dec, 10–35. For example, there is an indemnification clause that requires Petitioner to

[u]pon Apple’s request, defend, Apple, its directors, officers, employees, independent contractors and agents (each an “Apple Indemnified Party”) from any and all claims, losses, liabilities, damages, taxes, expenses and costs, including without limitation, attorneys’ fees and court costs (collectively, “Losses”), incurred by an Apple Indemnified Party and arising from or related to . . . any claims that Your Covered Product or the distribution, sale, offer for sale, use or importation of Your Covered Product (whether alone or as an essential part of a combination), Licensed Application Information, metadata, or Pass Information violate or infringe any third party intellectual property or proprietary rights;

Id. at 43. There is no evidence in this case that Apple has invoked its rights under this clause, nor has Patent Owner argued or explained how this clause

IPR2022-01094
Patent 8,620,039 B2

or the parties' actions before the Board and in the underlying district court litigation implicate a common law agency relationship between the parties. An agency relationship could potentially occur if Apple were to request Petitioner to step in and defend it. Yet Patent Owner has provided no argument or persuasive evidence that such is the case here. Apple has, in fact, committed to its own defense by filing its own IPR, e.g., IPR2022-00600, against Patent Owner. Moreover, compelling evidence provided by Petitioner in this case is exactly the opposite, as Petitioner avers under penalty of perjury in interrogatory responses that “[t]here have been no communications between Petitioners and Apple, directly or through counsel, relating to indemnification or obligation to indemnify based on assertion of. . . U.S. Patent No. 8,620,039) (*id.* at 11–12).” Ex. 1023, 8–9, 14.

We recognize that Apple may derive some benefit if additional claims of the '039 patent are determined to be unpatentable in this proceeding. This derived benefit does not, however, make Apple an RPI to this proceeding.

See WesternGeco LLC v. ION Geophysical Corp., 889 F.3d 1308, 1321 (Fed. Cir. 2018) (stating in the context of the broader concept of privity that “[a]s a general proposition, we agree with the Board that a common desire among multiple parties to see a patent invalidated, without more, does not establish privity”).

On the facts and evidence before us in this proceeding, it is the Agreement, analyzed here and in our Institution Decision that best explains the business relationship between the parties. The Agreement sets forth with reasonable clarity the specific expectations of the parties; mainly that (a) Petitioner is allowed “a limited license to use the Apple Software and Services provided to You under this Program to develop and test Your Applications on the terms and conditions set forth in this Agreement,” and

IPR2022-01094
Patent 8,620,039 B2

(b) “Applications that meet Apple’s Documentation and Program Requirements may be submitted for consideration by Apple for distribution via the App Store, Custom App Distribution, or for beta testing through TestFlight.” Ex. 2009, 1. Accordingly, the evidence leads us to conclude that Apple is a distributor of Petitioner’s App for use with Petitioner’s “Yale Smart Lock” products, and without more, that is about all that can be said about the relationship.

We turn, below, to particular facts in this case that Patent Owner argues the Board overlooked in our Institution Decision.

During oral argument Patent Owner’s counsel raised a specific issue concerning our earlier conclusion in our Institution Decision that Apple is *not* a real party in interest to this proceeding or a privy with Petitioner. Inst. Dec. 28; Tr. 45–46. Counsel contends “there is an inconsistency between [Petitioner’s], you know, assertions regarding Apple in the [Declaratory Judgment] complaint. And then in defending the RPI position.” Tr. 45:20–23. Specifically, counsel explained that they “didn’t see that the Board specifically considered our argument that it’s relevant that ASSA ABLOY filed the DJ complaint with respect to the 039 patent, even though the 039 patent had never been raised by Patent Owner to ASSA ABLOY.” *Id.* at 46:3–6. Counsel further argued that the present “situation mirror[s] the situation in the *Worlds v. Bungie* case, where a very similar fact pattern was considered relevant by the [F]ederal [C]ircuit.” *Id.* at 46:7–9; *see also* *Worlds Inc. v. Bungie, Inc.*, 903 F.3d 1237, 1239 (Fed. Cir. 2018) (“*Bungie*”) (determining that because “the Board erred in its real-party-in-interest analysis, we vacate its decisions and remand for proceedings consistent with this opinion”).

Our analysis of Patent Owner’s section 315(b) time bar arguments in our Institution Decision covers over 20 pages and considers in detail evidence submitted by both parties regarding business relationships and the Apple Developer License Agreement, i.e., the “Agreement,” (Ex. 2009) including warranties, indemnification, product inspection and insurance, between Petitioner and Apple. Inst. Dec. 10–35. For example, as it relates to Patent Owner’s issue raised here, we noted that “[i]n the Declaratory Judgment complaint, Petitioner states, ‘[CPC] is also engaged in an aggressive litigation campaign that includes Apple Inc. (‘Apple’), *a business partner* of [Petitioner].’” *Id.* at 15. We explained that

[t]he business relationship between Apple and Petitioner is that Petitioner, or one of the named entities collectively referred to as Petitioner, makes products that interface with Apple products and may be sold on Apple’s website. For example, ASSA ABLOY Residential Group, Inc., a named entity included as a Petitioner in this proceeding, makes and sells security locks under the brand name “Yale” . . . the Yale Assure Lock uses a software application (“App”) on one’s mobile phone, here on an iPhone sold by Apple, to lock and unlock doors. The App is developed by Petitioner, or one of its business partners, and distributed to iPhone users through the Apple App store.

Id. at 15–16. Thus, in our Institution Decision we did consider the fact that Petitioner, in its Declaratory Judgment Complaint, admitted to being a business partner with Apple. We also considered the fact that, as part of the business relationship, Petitioner entered into the Agreement. *Id.* at 16. We considered critical clauses in the Agreement, such as the representations and warranties clause explaining that “[w]e do *not* consider Section 3.2(d) to be a ‘warranty.’ It is not a guarantee that products will not infringe. It is a representation of the developer’s current ‘knowledge and belief.’ It is far

IPR2022-01094
Patent 8,620,039 B2

different from the obligations created by the App developer’s agreement in *Bungie*.” *Id.* at 20.

As discussed above, we determined that the Agreement did in fact contain an indemnification clause, which *could* be implemented “upon Apple’s request.” *Id.* at 23–26. However, also different from the facts in *Bungie*, in this case we have sworn interrogatories provided by Petitioner presenting strong evidence that “[t]here have been no communications between Petitioners and Apple, directly or through counsel, relating to indemnification or obligation to indemnify based on assertion of . . . U.S. Patent No. 8,620,039.” *Id.* at 26 (quoting Ex. 1023, 11–12).

Patent Owner now urges us to also consider the fact that its cease-and-desist letters to Petitioner, i.e., the “Yale Letters” (Exs. 2005, 2006), never threatened Petitioner with infringement of the ’039 patent, only U.S. Patent Nos. 9,665,705 and 9,269,208. *See* Prelim. Resp. 7 (Patent Owner arguing that it “never raised or otherwise mentioned the ’039 Patent to Yale or any of the Petitioners at any time.”) (citing Ex. 2008). This is a concern, Patent Owner contends, because Petitioner filed its Declaratory Judgment Complaint admitting to a business relationship with Apple as well as this IPR, and both proceedings challenge the ’039 patent. *See* Ex. 2007 ¶ 2 (Petitioner stating in its Declaratory Judgment Complaint that “[t]he ASSA ABLOY Entities seek a declaration of non-infringement of U.S. Patent Nos. 9,269,208 (“the ’208 Patent”), 9,665,705 (“the ’705 Patent”), and 8,620,039 (“the ’039 Patent”) (collectively, the “Patents-in-Suit”)).

This argument is frankly somewhat undeveloped in Patent Owner’s explanations of the facts and background in its Preliminary Response. Prelim. Resp. 5–10. We acknowledge that Petitioner was apparently never overtly threatened with infringement of the ’039 patent. Ex 2005; Ex. 2006.

IPR2022-01094
Patent 8,620,039 B2

Yet Patent Owner fails to persuasively explain *why* Petitioner's challenges to the '039 patent in the Declaratory Judgment Complaint weigh in favor of finding privy or a real party in interest relationship between Petitioner and Apple. *See* Prelim. Resp. 7 (Patent Owner arguing largely that "Patent Owner never raised or otherwise mentioned the '039 Patent to Yale or any of the Petitioners at any time."). As we understand the argument, Patent Owner alleges that because it never threatened Petitioner with the '039 patent, Petitioner is now, without provocation, doing Apple's bidding and working at Apple's behest by challenging the '039 patent in the Declaratory Judgment Complaint and in these *inter partes* review proceedings. It is also not clearly explained why the inclusion of Petitioner's related entities of ASSA ABLOY Global Solutions, Inc. ('Hospitality'), and HID Global Corporation, in these IPR proceedings as real parties in interest and also in the Declaratory Judgment Complaint, matters as to the relationship between Petitioner and Apple. *See* Prelim. Resp. 8 (arguing that "Petitioners also filed the Declaratory Judgment Complaint as to HID and Hospitality, whom Patent Owner had never contacted regarding the patents or technology at issue") (citing Ex. 2005; Ex. 2006; Ex. 2008).

Two things can be true, Petitioner can have a business relationship with Apple and both parties can have a legitimate interest in defending themselves separately in litigation. We do not find anything in Petitioner's Declaratory Judgment Complaint that alters our prior decision in this regard. The fact that Petitioner and each of its entities were not explicitly threatened with infringement allegations in the Yale Letters as to the '039 patent does not mean that Patent Owner would never assert infringement against Petitioner based on the '039 patent claims. Ex. 2005; Ex. 2006. This is especially true in light of the fact that Patent Owner asserted the '039 patent

IPR2022-01094
Patent 8,620,039 B2

against Apple in *CPC Patent Technologies Pty Ltd v. Apple Inc.*, No. 3:22-cv-02553, apparently due to or resulting from the products that Petitioner makes, uses, and sells through Apple's electronic device platforms.

Ex. 2007 ¶ 44 (“On February 23, 2021, [Patent Owner] asserted all three of the Patents-in-Suit against Apple.”).

On the facts here, we conclude that filing a declaratory judgment action or an *inter partes* review to challenge the claims of a patent, i.e., the '039 patent, that was asserted against a third party based on products made by Petitioner, is a reasonable litigation strategy for Petitioner independently. The declaratory judgment action filing itself does not demonstrate some sort of heightened collusion even where a benefit inures to a party with whom Petitioner has a business relationship. Patent Owner has not explained, for instance, that but for Apple's technology or actions, Petitioner has no actionable reason to challenge the patentability of the '039 patent claims.

See, generally, Prelim. Resp. Also, by way of example, Patent Owner argues in its Preliminary Response that in the Declaratory Judgment Complaint, “Petitioners further asserted that ‘it is highly likely that Charter Pacific will sue the Assa Abloy Entities *on the same patents that have been asserted against Apple.*’” Prelim. Resp. 22 (quoting Ex. 2007 ¶ 30). In our view, this assertion is primarily offered in the Complaint to show Petitioner’s apprehension of litigation because it admittedly makes, uses, and sells products potentially covered by the claims in the same three patents through Apple’s platforms. Patent Owner does not explain persuasively why Petitioner would not have been concerned about infringing the '039 patent, nor why such apprehension shows any more intimate relationship than we considered in our Institution Decision. The mere fact that an accused infringer, in this case Petitioner, files a declaratory judgment action

IPR2022-01094
Patent 8,620,039 B2

explaining its business relationship with Apple and offering reasons supporting the declaratory judgment action with respect to the same three patents that Apple is accused of infringing, does not, without more, establish persuasive additional information or substantive facts that we failed to consider in our original analysis.

Overall, and on the complete record before us, we do not find that any of Petitioner's assertions in its Declaratory Judgment Complaint change our underlying conclusion that Petitioner and Apple are not in privy or real parties in interest. *See* Inst. Dec. 34 (determining that “[t]he totality of the evidence before us does not establish anything other than a traditional business relationship between Apple and Petitioner.”).

III. CONCLUSION¹⁶

For the reasons discussed above, we determine Petitioner meets its burden of establishing, by a preponderance of the evidence, that the challenged claims are unpatentable, as summarized in the following table:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claims Not Shown Unpatentable
3, 4, 6–11, 15, 16, 18	103(a)	Sanford, Hsu	3, 4, 6–11, 15, 16, 18	

¹⁶ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

IPR2022-01094
Patent 8,620,039 B2

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claims Not Shown Unpatentable
3, 4, 6–11, 15, 16, 18	103(a)	Sanford, Hsu, Tsukamura ¹⁷		
5	103(a)	Sanford, Hsu, Leu	5	
5	103(a)	Sanford, Hsu, Leu, Tsukamura ¹⁸		
12	103(a)	Sanford, Hsu, Houvener	12	
12	103(a)	Sanford, Hsu, Tsukamura, Houvener ¹⁹		
17	103(a)	Sanford, Hsu, McCalley	17	

¹⁷ Because Petitioner’s contentions regarding the obviousness of claims 3, 4, 6–11, 15, 16, and 18 in view of Sanford and Hsu are dispositive of these challenged claims, we do not reach asserted ground 2. *See In re Gleave*, 560 F.3d 1331, 1338 (Fed. Cir. 2009).

¹⁸ Because Petitioner’s contentions regarding the obviousness of claim 5 in view of Sanford, Hsu and Leu are dispositive of these challenged claims, we do not reach asserted ground 4. *See In re Gleave*, 560 F.3d. at 1338.

¹⁹ Because Petitioner’s contentions regarding the obviousness of claim 12 in view of Sanford, Hsu and Houvener are dispositive of these challenged claims, we do not reach asserted ground 6. *See In re Gleave*, 560 F.3d. at 1338.

IPR2022-01094
Patent 8,620,039 B2

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claims Not Shown Unpatentable
17	103(a)	Sanford, Hsu, Tsukamura, McCalley ²⁰		

III. ORDER

For the reasons given, it is

ORDERED that, based on a preponderance of the evidence, claims 1, 2, 13, 14, 19, and 20 of the '039 patent have been shown to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, any party to the proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

²⁰ Because Petitioner's contentions regarding the obviousness of claim 17 in view of Sanford, Hsu and McCalley are dispositive of these challenged claims, we do not reach asserted ground 8. *See In re Gleave*, 560 F.3d. at 1338.

IPR2022-01094
Patent 8,620,039 B2

For PETITIONER:

Dion Bregman
Andrew Devkar
James Kritsas
MORGAN, LEWIS & BOCKIUS LLP
dion.bregman@morganlewis.com
andrew.devkar@morganlewis.com
james.kritsas@morganlewis.com

PATENT OWNER:

Andrew Ryan
CANTOR COLBURN LLP
aryan@cantorcolburn.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASSA ABLOY AB, ASSA ABLOY INC., ASSA ABLOY RESIDENTIAL GROUP, INC., AUGUST HOME, INC., HID GLOBAL CORPORATION, ASSA ABLOY GLOBAL SOLUTIONS, INC.,

Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY LTD.,
Patent Owner.

Case IPR2022-01093
Patent 8,620,039

PATENT OWNER'S NOTICE OF APPEAL

Pursuant to 37 C.F.R. §§ 90.2(a) and 90.3(b)(1), and 35 U.S.C. §§ 141, 142, and 319, timely notice is hereby provided that Patent Owner CPC Patent Technologies Pty Ltd. (“Patent Owner”) hereby appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision entered by the Patent Trial and Appeal Board (the “Board”) on January 31, 2024 (Paper 37) in *Inter Partes Review IPR2022-01093*, and from all other underlying or supporting orders, decisions, rulings, and opinions. A copy of said Final Written Decision is attached hereto.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), Patent Owner states that the issues on appeal may include, but are not limited to, the following, as well as any related findings, determinations, rulings, decisions, opinions, or other related issues:

- The Board’s determination that the challenged claims of U.S. Patent No. 8,620,039 are unpatentable; and
- The Board’s determination that the Petition is not time-barred under 35 U.S.C. § 315(b).

Patent Owner reserves the right to challenge any finding or determination supporting or related to the issues listed above and to challenge any other issues decided adversely to Patent Owner in the Final Written Decision and/or any underlying findings, determinations, rulings, decisions, or opinions.

Patent Owner is filing one copy of this Notice of Appeal with the Director of the United States Patent and Trademark Office, and a copy of this Notice of Appeal is being filed electronically with the Board. In addition, a copy of this Notice of Appeal is being electronically filed with the United States Court of Appeals for the Federal Circuit, along with the required docketing fee.

Respectfully submitted,

Dated: February 15, 2024

By: /Andrew C. Ryan/
Andrew C. Ryan
Reg. No. 43,070
Steven M. Coyle (*pro hac vice*)
Nicholas A. Geiger (*pro hac vice*)
CANTOR COLBURN LLP
20 Church Street, 22nd Floor
Hartford, CT 06103
Tel: (860) 286-2929
Fax: (860) 286-0115
ryan@cantorcolburn.com
scoyle@cantorcolburn.com

*Attorneys for Patent Owner
CPC Patent Technologies Pty Ltd.*

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 90.2(a)(1), on February 15, 2024 the foregoing Notice of Appeal was electronically filed with the Patent Trial and Appeal Board via the P-TACTS System in accordance with 37 C.F.R. § 42.6(b)(1), and mailed to the Director via Priority Mail Express in accordance with 37 C.F.R. §§ 1.10 and 104.2 at the following address:

Director of the U.S. Patent and Trademark Office
c/o Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Pursuant to 37 C.F.R. § 90.2(a)(2) on February 15, 2024, the foregoing Notice of Appeal was electronically filed with the Court of Appeals for the Federal Circuit via CM/ECF with requisite fees paid via pay.gov.

Pursuant to 37 C.F.R. § 42.6(e) and the parties' agreement to accept electronic service, on February 15, 2024, the foregoing Notice of Appeal was served via email on the following counsel of record for Petitioners:

Dion Bregman
Andrew Devkar
James J. Kritsas
Morgan, Lewis & Bockius LLP
1400 Page Mill Road
Palo Alto, CA 94304
HID-IPRs@morganlewis.com

Dated: February 15, 2024

By: /Andrew C. Ryan/
Andrew C. Ryan (Reg. 43,070)

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASSA ABLOY AB, ASSA ABLOY INC., ASSA ABLOY RESIDENTIAL GROUP, INC., AUGUST HOME, INC., HID GLOBAL CORPORATION, ASSA ABLOY GLOBAL SOLUTIONS, INC.,

Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY LTD.,
Patent Owner.

Case IPR2022-01094
Patent 8,620,039

PATENT OWNER'S NOTICE OF APPEAL

Pursuant to 37 C.F.R. §§ 90.2(a) and 90.3(b)(1), and 35 U.S.C. §§ 141, 142, and 319, timely notice is hereby provided that Patent Owner CPC Patent Technologies Pty Ltd. (“Patent Owner”) hereby appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision entered by the Patent Trial and Appeal Board (the “Board”) on January 31, 2024 (Paper 35) in *Inter Partes* Review IPR2022-01094, and from all other underlying or supporting orders, decisions, rulings, and opinions. A copy of said Final Written Decision is attached hereto.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), Patent Owner states that the issues on appeal may include, but are not limited to, the following, as well as any related findings, determinations, rulings, decisions, opinions, or other related issues:

- The Board’s determination that the challenged claims of U.S. Patent No. 8,620,039 are unpatentable; and
- The Board’s determination that the Petition is not time-barred under 35 U.S.C. § 315(b).

Patent Owner reserves the right to challenge any finding or determination supporting or related to the issues listed above and to challenge any other issues decided adversely to Patent Owner in the Final Written Decision and/or any underlying findings, determinations, rulings, decisions, or opinions.

Patent Owner is filing one copy of this Notice of Appeal with the Director of the United States Patent and Trademark Office, and a copy of this Notice of Appeal is being filed electronically with the Board. In addition, a copy of this Notice of Appeal is being electronically filed with the United States Court of Appeals for the Federal Circuit, along with the required docketing fee.

Respectfully submitted,

Dated: February 15, 2024

By: /Andrew C. Ryan/
Andrew C. Ryan
Reg. No. 43,070
Steven M. Coyle (*pro hac vice*)
Nicholas A. Geiger (*pro hac vice*)
CANTOR COLBURN LLP
20 Church Street, 22nd Floor
Hartford, CT 06103
Tel: (860) 286-2929
Fax: (860) 286-0115
ryan@cantorcolburn.com
scoyle@cantorcolburn.com

*Attorneys for Patent Owner
CPC Patent Technologies Pty Ltd.*

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 90.2(a)(1), on February 15, 2024 the foregoing Notice of Appeal was electronically filed with the Patent Trial and Appeal Board via the P-TACTS System in accordance with 37 C.F.R. § 42.6(b)(1), and mailed to the Director via Priority Mail Express in accordance with 37 C.F.R. §§ 1.10 and 104.2 at the following address:

Director of the U.S. Patent and Trademark Office
c/o Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Pursuant to 37 C.F.R. § 90.2(a)(2) on February 15, 2024, the foregoing Notice of Appeal was electronically filed with the Court of Appeals for the Federal Circuit via CM/ECF with requisite fees paid via pay.gov.

Pursuant to 37 C.F.R. § 42.6(e) and the parties' agreement to accept electronic service, on February 15, 2024, the foregoing Notice of Appeal was served via email on the following counsel of record for Petitioners::

Dion Bregman
Andrew Devkar
James J. Kritsas
Morgan, Lewis & Bockius LLP
1400 Page Mill Road
Palo Alto, CA 94304
HID-IPRs@morganlewis.com

Dated: February 15, 2024

By: /Andrew C. Ryan/
Andrew C. Ryan (Reg. 43,070)